Konkrete algebraiske strukturer 4-6

Madsen, Anders J. Hede

Publication date:
2006

Document Version
Også kaldet Forlagets PDF

Citation for published version (APA):
Madsen, A. J. H. (2006). *Konkrete algebraiske strukturer 4-6*. Roskilde Universitet. IMFUFA-tekst : i, om og med matematik og fysik Nr. 455 http://milne.ruc.dk/ImfufaTekster/

IMFUFA tekst

- I, OM OG MED MATEMATIK OG FYSIK

Konkrete algebraiske strukturer 4-6

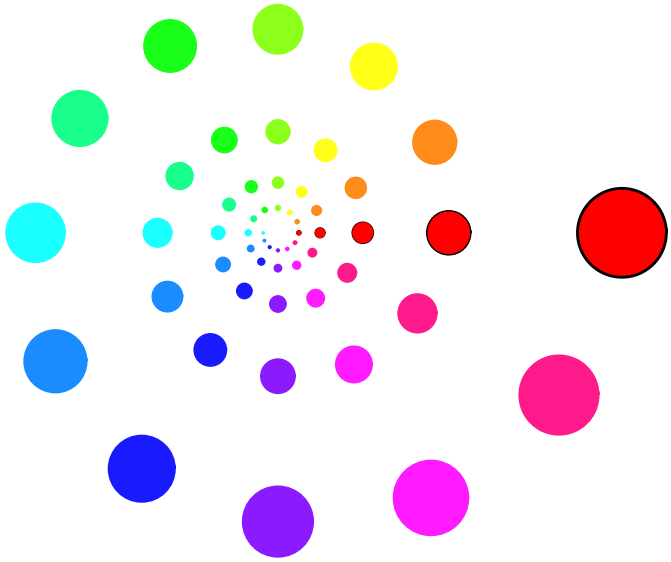
Anders Madsen

december 2006

nr. 455 - 2006

-

Anders Madsen



KONKRETE ALGEBRAISKE STRUKTURER 4–6

IMFUFAtekst 455

Dette nummer af IMFUFAtekster omfatter tre hæfter i en serie med titlen "Konkrete algebraiske strukturer", som jeg har skrevet til algebrakurset (E1) på matematikuddannelsen ved IMFUFA på RUC. Det drejer sig om

4: Ringe af hele tal 5: Legemer og vektorrum 6: Permutationer

Hæfterne skal ses i sammenhæng med en anden serie hæfter med titlen "Abstrakte algebraiske strukturer". Disse to serier udgør hver sin kæbe i en knibtang.

Naturligvis ville det være tomt (og frustrerende) at undervise i abstrakt algebra uden inddragelse af konkrete eksempler og det ville være fattigt (og perspektivforladt) kun at gennemgå konkrete eksempler uden at inddrage de underliggende abstrakte strukturer.

På den anden side er der en vis skønhed i at fremhæve den abstrakte karakter ved at isolere den og lade dens top-down karakter fremstå tydeligt som i det forkætrede forbillede "Matematikens elementer" af Bourbaki. Starte med de groveste strukturer og efterhånden tilføje finere strukturelementer. Alle resultater, som går igen og igen, formuleres og bevises en gang for alle.

Ligeledes er der en tilfredsstillelse forbundet med at lade de enkelte konkrete strukturer stå så enkelt som muligt, uden overflødige dikkedarer, das Ding an sich. Og der er fornøjelsen ved at se det essentielt samme argument komme igen og igen i forskellige forklædninger.

Udover den æstetiske tilfredstillelse ved den rene abstraktion og den rene fornøjelse ved de konkrete detaljer har begge disse perspektiver en stor erkendelsesmæssig betydning og bidrager til udviklingen af kompetencer som er væsentlige for matematikere.

Jeg har valgt at fremhæve de to modsatrettede men samspillende perspektiver ved den opdeling som de to serier repræsenterer. De enkelte konkrete strukturer er fremstillet i enkeltstående fremstillinger uden indbyrdes referencer. Stof som forudsættes flere steder er medtaget hvert sted. Men udvalget af detaljer er foretaget på en sådan måde at det bedst muligt kan levere stof til den abstrakte del.

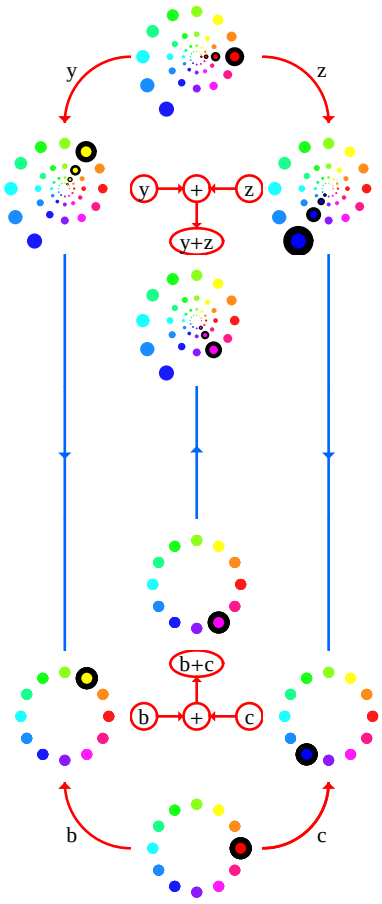
Den matematiske kerne for de enkelte hæfter, uden forbindende tekst og illustrationer, har foreligget tidligere i mere rå form beregnet på uddybning ved forelæsning og ikke egnet til selvstudium, ikke mindst på grund af utallige trykfejl og tanketorsk, som de studerende med stor tålmodighed har fanget. Dette skylder jeg dem tak for og derfor er hæfterne tilegnet alle tidligere og nuværende studerende på E1, som jeg takker for deres medvirken.

Anders Madsen, december 2006

IMFUFA tekst nr 455/2006 - 104 sider — ISSN : 0106-6242

Anders Madsen

RINGE AF HELE TAL



KONKRETE ALGEBRAISKE STRUKTURER

4

Dette er et hæfte i en serie med titlen "Konkrete algebraiske strukturer", som jeg har skrevet til algebrakurset (E1) på matematikuddannelsen ved IMFUFA på RUC.

Hæfterne skal ses i sammenhæng med en anden serie hæfter med titlen "Abstrakte algebraiske strukturer". Disse to serier udgør hver sin kæbe i en knibtang.

Naturligvis ville det være tomt (og frustrerende) at undervise i abstrakt algebra uden inddragelse af konkrete eksempler og det ville være fattigt (og perspektivforladt) kun at gennemgå konkrete eksempler uden at inddrage de underliggende abstrakte strukturer.

På den anden side er der en vis skønhed i at fremhæve den abstrakte karakter ved at isolere den og lade dens top-down karakter fremstå tydeligt som i det forkætrede forbillede "Matematikens elementer" af Bourbaki. Starte med de groveste strukturer og efterhånden tilføje finere strukturelementer. Alle resultater, som går igen og igen, formuleres og bevises en gang for alle.

Ligeledes er der en tilfredsstillelse forbundet med at lade de enkelte konkrete strukturer stå så enkelt som muligt, uden overflødige dikkedarer, das Ding an sich. Og der er fornøjelsen ved at se det essentielt samme argument komme igen og igen i forskellige forklædninger.

Udover den æstetiske tilfredstillelse ved den rene abstraktion og den rene fornøjelse ved de konkrete detaljer har begge disse perspektiver en stor erkendelsesmæssig betydning og bidrager til udviklingen af kompetencer som er væsentlige for matematikere.

Jeg har valgt at fremhæve de to modsatrettede men samspillende perspektiver ved den opdeling som de to serier repræsenterer. De enkelte konkrete strukturer er fremstillet i enkeltstående fremstillinger uden indbyrdes referencer. Stof som forudsættes flere steder er medtaget hvert sted. Men udvalget af detaljer er foretaget på en sådan måde at det bedst muligt kan levere stof til den abstrakte del.

Den matematiske kerne for de enkelte hæfter, uden forbindende tekst og illustrationer, har foreligget tidligere i mere rå form beregnet på uddybning ved forelæsning og ikke egnet til selvstudium, ikke mindst på grund af utallige trykfejl og tanketorsk, som de studerende med stor tålmodighed har fanget. Dette skylder jeg dem tak for og derfor er hæfterne tilegnet alle tidligere og nuværende studerende på E1, som jeg takker for deres medvirken.

Hefterne findes i netudgaver med alle referencer som aktive links og med opdateringer:

Anders Madsen, december 2006

Indholdsfortegnelse

1: Prolog

I dette hæfte skal du møde forskellige konkrete eksempler på algebraiske strukturer. Vi taler om en algebraisk struktur, når vi har en bestemt type objekter og en eller flere operationer på denne type objekter, der fører til et objekt af samme type, samt nogle regneregler for disse operationer.

Det mest oplagte eksempel har som objekter de reelle tal, som operationer de sædvanlige aritmetiske operationer med de sædvanlige regneregler.

Hæftet handler om de hele tal og om de mest elementære definitioner og egenskaber for de hele tals algebra, som udspringer de tre elementære regneoperationer addition, subtraktion og multiplikation. Desuden inddrages disse operationers relation til tallenes ordning efter størrelse.

Denne algebraiske struktur er et hovedeksempel på en ring, en abstrakt algebraiske struktur. En ring generaliserer strukturer med addition og multiplikation, hvor additionen har en modsat operation subtraktion, men hvor der ikke findes en division som modsat operation for multiplikation.

Fremstillingen er dog helt konkret. Men du vil få fornøjelse af denne konkrete algebraiske struktur, når du en gang møder den abstrakte.

Et hovedpunkt bliver division med rest, som må træde i stedet for egentlig division. Der vil være en opsamling med tydeligørelse af den røde tråd i epilogen.

2: Divisorer og multipla

2.1: Forberedelser

Vi vil imidlertid ikke begynde helt fra bunden. Vi vil ikke definere hverken hvad et helt tal er eller hvordan regneoperationerne er defineret. Vi vil tværtimod tage både tallene og operationerne for givne. Men vi vil præcisere lidt nøjere hvad det er for regler vi tager for givne, således at vi ved en senere lejlighed kan nøjes med netop at bringe det angivne grundlag i orden. Med hele tal menes mængden $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

Lad os da antage, at vi af vor herre har fået foræret operationerne addition, subtraktion og multiplikation, således at addition og multiplikation er kommutative, associative operationer, og at subtraktion er den modsatte operation

til addition. Vi går også ud fra at multiplikationen er distributiv mht addition, hvoraf man udleder reglerne for at gange ind i parenteser på de velkendte måder. Vi vil også uden kvababbelse benytte forkortningsreglen, som siger at man kan fjerne eller tilføje den samme faktor på begge sider af et lighedstegn uden at ligningen mister sin gyldighed. Faktoren må dog ikke være nul.

Vi antager endvidere at enhver delmængde, for hvilken der findes en majorant (dvs et tal som er større end alle mængdens tal), også har et maksimum, (dvs et element i mængden som er større end alle dens øvrige elementer), og at enhver delmængde som har en minorant også har et minimum. Denne antagelse kan dog let bevises ved induktion. Vi vil i øvrigt uden bæven benytte os af induktionsbeviser.

Vi regner også med mængder.

Lad os inden vi går rigtigt igang udvide regneoperationerne til også at kunne anvendes på delmængder. Dette gøres på helt oplagt måde. Vi kan nøjes med et par eksempler:

$$A+B=\{a+b : a\in A, b\in B\},\quad kA=\{ka : a\in A\},\quad (A,B\subset\mathbb{Z}, k\in\mathbb{Z}).$$

Vi kan se at $3\mathbb{Z}$ er mængden $\{\ldots,-6,-3,0,3,6,\ldots\}$, som vi passende kalder den dobbeltsidet uendelige 3-tabel. Vi vil referere til den som 3-tabellen.

Man kan udlede en række regler for disse udvidede operationer, hvad vi dog ikke går i detaljer med her. At man dog må jo tænke sig om, illustreres af formlen $\mathbb{Z}+\mathbb{Z}=\mathbb{Z}$.

2.2: Definitioner og notation

Vi starter med den multiplikative struktur

Noget af de mest karakteristiske for de hele tal er knyttet til at division er en operation, som langt fra altid er mulig. Men noget kan man jo trods alt.

Som bekendt siger vi at b er et *multiplum* af a hvis b tilhører a-tabellen, altså hvis $b\in a\mathbb{Z}$, hvilket vi også udtrykker ved at sige at a er en *divisor* i b. Vi benytter skrivemåden $a|b$ for denne relation.

Vi benytter på oplagt måde betegnelserne *delelig* og *delelighed* i overensstemmelse med de her givne definitioner. Man kan også møde de gamle danske udtryk *mangefold* og *deler* for henholdsvis multiplum og divisor.

Bemærk at med disse definitioner, som er udvidede i forhold til de naive, der kun omfatter positive tal, vil 0 være multiplum af hvad som helst, og hvad som helst vil følgelig være divisor i 0. Men 0 er dog kun divisor i sig selv. Lad os sammenfatte i

1. Sætning: Kriterium for delelighed.

$a|b \Leftrightarrow b\mathbb{Z} \subseteq a\mathbb{Z}$

Beviset er en øvelse (Ø1). E2 Ø3

Hvis $A \subset \mathbb{Z}$ så siger vi at a er en fælles divisor for A, hvis a er divisor i alle elementer i A. Der vil oplagt(!) altid findes en største fælles divisor for en ikke tom delmængde A og for den vil vi anvende benævnelserne $\bigsqcap A$, sfd$A$, gcd$A$, (**s**tørste **f**ælles **d**ivisor, **g**reatest **c**ommon **d**ivisor). Tilsvarende defineres mindste fælles multiplum for en mængde A og denne skrives $\bigsqcup A$. (Eller mfm og lcm).

Hvis $A = \{a_1, \ldots, a_n\}$ skriver vi også $a_1 \sqcap \ldots \sqcap a_n$ eller sfd$(a_1, \ldots, a_n)$ og analogt med mindste fælles multiplum. E4 Ø5

2. Sætning: Multiplikation af største fælles divisor

Hvis $k > 0$ da gælder at $(ka) \sqcap (kb) = k(a \sqcap b)$

Beviset er en øvelse (Ø6).

2.3: Division med rest.

Vi må inddrage den additive struktur

Hvis $a|b$ kan vi udføre divisionen og definere kvotienten $\frac{b}{a}$. For denne kun delvist definerede operation gælder mange af de sædvanlige regneregler. Det går vi ikke i detaljer med. Lad os som et eksempel nævne at

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

forstået på den måde, at hvis begge sider er veldefinerede, da er de ens.

I de fleste situationer går divisionen imidlertid ikke op. For at klare dette problem må vi have den additive struktur (addition og subtraktion) med ind i billedet. Når vi vil vide om b går op i a foretager vi succesive subtraktioner af

b indtil vi ikke kan mere. (Denne anvendelse af subtraktion til behandling af et multiplikativt problem er naturligvis blot et udtryk for at multiplikation er en form for successiv addition med samme tal.)

Dette er jo hvad vi kalder division med rest. Her vil vi bruge rest som betegnelse for noget der er blevet til rest når vi har subtraheret b et antal gange:

---

3. Definition: Rest

Lad $a, b, r \in \mathbb{Z}$. Vi siger at r er en rest af a modulo b, hvis der findes $q \in \mathbb{Z}$ således at $a = bq + r$. Vi siger da også a har r som rest modulo b. Vi benytter betegnelsen $[a]_b$ for mængden af rester af a modulo b, som vi også kalder restklassen for a modulo b.

E7 Ø8

Sprogligt set betyder *modulo* (som er latin)nærmest "med hensyn til". Det benyttes ofte i matematisk talebrug, også i andre betydninger end den her givne, som jo er præcist fastlagt.

4. Sætning: Karakterisering af klassen af rester.

---

r er en rest af a modulo b hvis og kun hvis $r \in a + b\mathbb{Z}$, altså $[a]_b = a + b\mathbb{Z}$.

Beviset er en øvelse.

Resterne af a modulo b er altså en parallelforskudt b-tabel.

5. Sætning: Eksistens af principal rest

Lad $a, b \in \mathbb{Z}$ og antag at $b > 0$(!) da findes der netop en rest r af a modulo b som opfylder at $0 \leq r < b$

Bevis : Mængden af ikke-negative rester har en minorant, nemlig 0 og derfor også et minimum, lad dette være r. Da må $r < b$ thi ellers ville $r - b$ være en ikke-negativ rest som var mindre end r, i modstrid med definitionen af r.

---

6. Definition: Principal rest

Den i foregående sætning (S 5) nævnte rest kaldes den principale rest af a modulo b og betegnes $a \bmod b$.

E9 Ø10 Ø11

---

7. Definition: Heltalskvotient

Lad $a = bq + r$, hvor $r = a \bmod b$. Vi kalder da q for heltalskvotienten af a ved division med b og benævner den a div *b.*

Vi har altså at $a = (a \text{ div } b)b + (a \bmod b)$

Ø12

2.4: Euklids algoritme

Vi vil vende tilbage til studiet af divisorer, idet vi vha af division med rest nu kan formulere følgende slagkraftige algoritme til bestemmelse af største fælles divisor. Denne algoritme har været kendt i over 2000 år. Den stammer fra den græske storhedstid i matematikken.

Algoritmen bygger på følgende

8. Sætning: Forberedelse til Euklid

Hvis $a = bq + r$ da er $a \sqcap b = b \sqcap r$

Bevis : Vi bemærker først at en divisor i to tal også er divisor i deres sum. Når dette benyttes på de to summer $r = a + (-bq)$ og $a = bq + r$ ses at et tal c er fælles divisor for a og b hvis og kun hvis c også en fælles divisor for b og r.

9. Sætning: Euklids algoritme

Følgende rekursivt definerede funktion Euklid *er veldefineret og bestemmer $a \sqcap b$ for alle a og alle $b \geq 0$:*

$$\text{Euklid}(a,b) = \begin{cases} |a| & \textit{hvis } b = 0 \\ \text{Euklid}\textit{(b,r), hvor } a = bq + r, 0 \leq r < b & \textit{hvis } b > 0 \end{cases}$$

Bevis : *Vi fører beviset ved induktion efter b.*

Påstanden er klart rigtig hvis $b = 0$.

Lad så $b > 0$. Vi antager at vi har bevist påstanden i sætningen for alle par (a', b') med $b' < b$. og vil vise at den så også gælder for $b' = b$. Vi kan indledningsvis, da $b > 0$ bestemme q, r således at $a = bq + r, 0 \leq r < b$. Når vi da sætter $(a', b') = (b, r)$ så har vi åbenbart at $b' < b$. Så $b \sqcap r = \text{Euklid}(b, r)$. Men af S8 følger jo at $a \sqcap b = b \sqcap r$. Vi har så at påstanden i sætningen også gælder for b.

	a	b	r	$a = bq + r$	q	x	y
1	130	48	34	$130 = 48 \cdot 2 + 34$	2	-7	19
2	48	34	14	$48 = 34 \cdot 1 + 14$	1	5	-7
3	34	14	6	$34 = 14 \cdot 2 + 6$	2	-2	5
4	14	6	2	$14 = 6 \cdot 2 + 2$	2	1	-2
5	6	2	0	$6 = 2 \cdot 3 + 0$	3	0	1
6	2	0				1	0

	q	x	y	$x'b + y'(a - qb) = xa + yb$
1	2	-7	19	$5 \cdot 48 + (-7)(130 - 2 \cdot 48) = (-7) \cdot 130 + 19 \cdot 48$
2	1	5	-7	$(-2) \cdot 34 + 5(48 - 1 \cdot 34) = 5 \cdot 48 + (-7) \cdot 34 =$
3	2	-2	5	$1 \cdot 14 + (-2)(34 - 2 \cdot 14) = (-2) \cdot 34 + 5 \cdot 14 =$
4	2	1	-2	$0 \cdot 6 + 1(14 - 2 \cdot 6) = 1 \cdot 14 + (-2) \cdot 6 =$
5	3	0	1	$1 \cdot 2 + 0(6 - 3 \cdot 2) = 0 \cdot 6 + 1 \cdot 2 =$
6	1	0		

Tabel til Euklids algoritme. Tabellen er skåret over på midten (vertikalt)

Ved anvendelse af algoritmen gås altså frem på følgende måde, idet der henvises til skemaets forreste 6 søjler:

Første række udfyldes med de givne værdier af a og b. Divisionen udføres, hvorved q og r bestemmes. Nu er første række færdigbehandlet.

Herefter fortsættes induktivt. Antag at vi i processen er nået til en bestemt række, som vi kalder den aktuelle. Fra den foregående række, som er færdig, aflæses b og r som indsættes som henhodsvis a og b i den aktuelle række og vi gør denne række færdig på samme måde som første række. Vi fortsætter på denne måde indtil vi har en række med $b = 0$. Da er vi nemlig færdige, og resultatet af algoritmen er da det a som står i samme række.

Alle informationerne er i øvrigt indeholdt i kolonnen med $a = bq + r$, og man kan naturligvis nøjes med at udfylde denne. De andre kolonner tjener her mere til at fremhæve systemet. Ø13

2.5: En fundamental formel for største fælles divisor.

I mange sammenhænge vil det (pudsigt nok) vise sig nyttigt at kunne udtrykke $a \sqcap b$ som en linearkombination af a og b med heltallige koefficienter. Derfor følgende måske lidt overraskende sætning, som vi formulerer som en algoritme til bestemmelse af de nævnte koefficienter.

10. Sætning: Euklids udvidede algoritme

Følgende rekursivt definerede funktion EuklidU *er veldefineret og bestemmer* $x, y \in \mathbb{Z}$ *således at* $a \sqcap b = xa + yb$*:*

$$\text{EuklidU}(a,b) = \begin{cases} (1,0) & & \text{hvis } b = 0 \\ \text{(y',x'-qy')}, & \text{hvor } a = bq+r,\ 0 \le r < b, \\ & (x', y') = \text{EuklidU}(b, r) & \text{hvis } b > 0 \end{cases}$$

Bevis : *Påstanden i sætningen er klart rigtig hvis* $b = 0$*, idet* $a \sqcap 0 = a = 1a + 0b$*.*

Lad så $b > 0$*.*

Vi gennemfører nu et induktionsbevis med induktion efter b*. Vi bemærker at vi netop har vist at sætningen gælder når* $b = 0$*, hvilket er første skridt.*

Vi antager derefter at vi har bevist at påstanden i sætningen for alle par (a', b') *med* $b' < b$*. Når vi da bestemmer* b, q, r *således at* $a = bq + r, 0 \le r < b$ *og dernæst sætter* $(a', b') = (b, r)$ *så har vi åbenbart at* $b' < b$ *og vi kan bruge algoritmen til at bestemme* (x', y') *således at* $b \sqcap r = a' \sqcap b' = x'b + y'r$*. Af ligningen* $a = bq + r$ *fås* $r = a - bq$*, som ved indsættelse giver at* $b \sqcap r = x'b + y'(a - bq) = y'a + (x' - qy')b$*. Hvis vi så sætter* $x = y'$ *og* $y = x' - qy'$ *så har vi at* $a \sqcap b = b \sqcap r = xa + yb$*, og det var jo det vi skulle bevise.*

Denne algoritme er endda let at implementere, hvilket skulle fremgå af de bagerste søjler i skemaet til illustration af den simple algoritme.

Når vi skal anvende den udvidede algoritme skal vi udføre skridtene i den simple først. Vi udfylder derefter det der mangler i hver række, men nedefra. Vi kan

starte i den tredjenederste række. Her har vi at $a \sqcap b = r = a - qb$ og vi skal derfor blot vælge $x = 1$ og $y = -q$.

Herefter fortsættes opad gennem rækkerne.

Antag at vi er nået til en bestemt række, hvor alle underliggende rækker er ordnede. Vi kalder denne for den aktuelle. Vi lader x', y' betegne værdierne i rækken under den aktuelle og sætter $x = y'$ og $y = x' - qy'$, hvor q aflæses i den aktuelle række. Når vi er nået til første række er vi færdige og kan aflæse resultatet som (x, y).

Alle informationerne i forbindelse med den udvidede algoritme er indeholdt i den sidste søjle og man kan derfor nøjes med at udføre denne. Bemærk at lighedstegnet i slutningen af hver række peger på rækken ovenover. De andre kolonner tjener her mere til at understrege systemet.

Ø14

Denne sætning, som har mange anvendelser, sætter lyset på tallene af formen $xa + yb$, hvor a og b er konstante og x og y gennemløber alle hele tal. Vi kan kort skrive mængden som $a\mathbb{Z} + b\mathbb{Z}$, altså summen af to tabeller. Vi kan nu give en overraskende karakterisering af denne mængde.

11. Sætning: Sum af tabeller er en tabel

$a\mathbb{Z} + b\mathbb{Z} = (a \sqcap b)\mathbb{Z}$

Bevis : Per definition er både a og b multipla af $a \sqcap b$, hvilket $xa + yb$ så også er. Dermed ses at $a\mathbb{Z} + b\mathbb{Z} \subseteq (a \sqcap b)\mathbb{Z}$

Vi kan vælge x, y så $(a \sqcap b) = xa + yb$. For ethvert $k \in \mathbb{Z}$ har vi da at $k(a \sqcap b) = kxa + kyb \in a\mathbb{Z} + b\mathbb{Z}$. Dette giver den modsatte inklusion.

Tænk over om dette resultat virker indlysende. Det bygger i hvert fald på en sætning (S10) som synes knapt så indlysende. Af sætningen følger f.eks. at ethvert tal kan skrives som sum af et tal fra 5-tabellen og et fra 12-tabellen. Hvordan ville du argumentere direkte for det. Det kunne du godt lige tænke over.

3: Primtal og primtalfaktorisering.

3.1: Primtal, definition og simple egenskaber

Primtal.

Vi vil nu koncentrere os om den multiplikative struktur. Hvordan kan tallene bygges op ved brug af multiplikation, hvad er atomerne (de mindste byggestene) og hvordan kan molekyler spaltes i atomer. Atomerne er primtallene og spaltningen er udtrykt i sætningen om entydig primfaktorisering. Efter definitionerne følger de værktøjer der skal bruges i forbindelse med spaltningen.

---

12. Definition: Primisk

Vi siger at a og b er indbyrdes primiske hvis $a \sqcap b = 1$.

På engelsk benyttes "coprime" for indbyrdes primisk.

---

13. Definition: Primtal

Et tal p som er større end 1 kaldes et primtal, hvis tallene $\{\pm 1, \pm p\}$ er dets eneste divisorer.

---

14. Sætning: Der findes ikke noget største primtal.

Mængden af primtal er uendelig.

Bevis : Følgende bevis findes hos Euklid.

Det er indirekte.

Antag at primtallene kan opstilles i en endelig følge $p_1 < \ldots < p_n$. Lad q betegne tallet $p_1 \cdots p_n + 1$. Da vil q være et primtal eller et sammensat tal. Hvis q er et primtal har vi en oplagt modstrid. Hvis q er et sammensat tal så må q have mindst en primfaktor. Men denne kan ikke optræde på listen, da ingen af dem som er på listen kan være divisor i q, da division med dem giver resten 1. Vi har altså fundet et primtal som ikke er med på listen, i strid med antagelsen.

Nu gør vi klar til hovedsætningen om primfaktorisering. Først en lille nyttig observation

15. Sætning: Primtal er indbyrdes primiske med alt, bortset fra egne multipla.

Antag at primtallet p ikke er divisor i a, da er p og a indbyrdes primiske.

Bevis : Sæt $b = p \sqcap a$. Hvis det gjaldt at $b > 1$ så måtte b som divisor i p være lig med p. Men så skulle p jo også gå op i a. Altså må $b = 1$, og altså må p og a være indbyrdes primiske.

Denne observation benyttes i følgende hovedhjælpemiddel, som også hviler på karakteriseringen af største fælles divisor som heltalslinearkombination.

16. Sætning: Primtal går op i mindst en faktor

Hvis primtallet p er divisor i produktet $a_1 \cdots a_n$ da er det divisor i mindst en af faktorerne.

Bevis : Induktion efter n. For $n = 1$ er det klart. Lad $n > 1$ og antag at sætningen er vist for færre end n faktorer. Hvis $p|a_1$ er der ikke mere at bevise. I modsat fald vil $p \sqcap a_1 = 1$ og vi kan således finde x, y således at $xa_1 + yp = 1$ (S10).

Vi har da at $a_2 \cdots a_n = (xa_1 + yp)a_2 \cdots a_n = xa_1 \cdots a_n + ypa_2 \cdots a_n$ Her af ses at p går op i $a_2 \cdots a_n$, idet p går op i $xa_1 \cdots a_n$ efter antagelsen i sætningen og p klart går op i $ypa_2 \cdots a_n$. Men nu får vi jo af induktionsanatagelsen at så må p gå op i en af faktorerne i $a_2 \cdots a_n$.

Lidt uklart udtrykt siger sætningen at et primtal ikke kan fordele sin gåen op i et produkt på forskellige faktorer.

Du vil muligvis undre dig over at sætningen kræver et så forholdsvis kompliceret bevis. Men så kan du jo prøve at omsætte din intuition til et simplere.

Bemærk at $6|3 \cdot 4$. (Hvad er det bemærkelsesværdige ved det?)

3.2: Primfaktorisering.

17. Sætning: eksistens af primfaktorisering.

Lad $a \in \mathbb{Z}, a > 1$. Der findes da en entydigt bestemt endelig følge af primtal $p_1 \leq \ldots \leq p_n$ således at $a = p_1 \cdots p_n$

Bevis : Induktion efter a.

Sagen er klar for $a = 2$.

Antag nu at betingelsen i sætningen er opfyldt for ethvert tal b, for hvilket $b < a$. Vi vil vise at betingelsen da også er opfyldt for a.

Hvis a er et primtal er sagen jo oplagt. Hvis a er sammensat lader vi p være en primfaktor i a og sætter $b = a/p$. Da er $b < a$. Efter induktionsantagelsen kan vi da finde primtallene $p_1, \ldots, p_n$ således at $b = p_1 \cdots p_n$. Vi danner nu mængden bestående af disse primtal og p, og ordner den efter størrelse. Hvis den ordnede liste er $q_1, \ldots, q_m$ er det klart at a er produkt af disse.

Så kommer vi til entydigheden.

Antag nu at $a = p_1 \cdots p_n$ og $a = q_1 \cdots q_m$ er to sådanne fremstillinger. Da p_1 går op i a, har vi at p_1 går op i $q_1 \cdots q_m$ og ifølge S16 må der så findes mindst et $i \leq m$ således at p_1 går op i q_i. Ved fortsættelse af dette argument fås at $\{p_1, \ldots p_n\} \subseteq \{q_1, \ldots, q_m\}$. Ved symmetri ses at også den modsatte inklusion holder. Det er altså de samme primfaktorer som indgår i begge fremstillinger. Vi mangler da blot at se at de optræder med det samme antal faktorer på begge sider. Men dette kan ses ved lidt opfindsom brug af forkortning.

Det samme primtal kan godt forekomme mere end en gang i primfaktoriseringen og kan da naturligt samles til en potens af primtallet. Opspaltningen for da formen $p_1^{e_1} \cdots p_n^{e_n}$, hvor $p_1, \ldots, p_n$ er de i faktoriseringen forekommende primtal.

Vi lader nu i stedet for p_n betegne det n-te af alverdens primtal ordnet efter størrelse. Hvis vi tillader eksponenten 0, da er ethvert tal karakteriseret ved at der for hvert n er givet en eksponent e_n, nemlig 0 hvis p_n ikke optræder i opspaltningen og ellers den eksponent som p_n optræder med. Denne følge af eksponenter indeholder al information om faktoriseringen. Den er bekvem når man skal sammenligne forskellige tal vha af deres opspaltning.

3.3: Primspektrum

18. Sætning: Forberedelse til primspektrum

Lad $a \in \mathbb{Z}, a > 0$. Lad p_n betegne det n-te primtal i følgen af alle primtal ordnet efter størrelse. Der findes da en entydigt bestemt følge (e_n) af ikke negative tal med følgende egenskaber:

Der findes et største indeks n for hvilket $e_n > 0$, kaldet det sidste betydende index.

For alle indeks n som er større end det sidste betydende indeks gælder det at $a = p_1^{e_1} \cdots p_n^{e_n}$

Bevis : Hvis $a = 1$ lader vi alle eksponenter være 0. Antag nu at $a > 1$. For de primtal p der forekommer i primfaktoriseringen af a lader vi den tilhørende eksponent være det antal gange som faktoren forekommer. For alle andre lader vi eksponenten være 0.

---

19. Definition: Primpektrum

Den i sætningen nævnte følge kalder vi for primspektret for a og betegner med $\sigma(a)$.

Betegnelsen primspektrum har jeg været nødt til selv at finde på, da jeg ikke kender nogen standardbetegnelse. Primspektret er ikke andet end et kompakt udtryk for primfaktoriseringen. At vi ønsker at arbejde med en uendelig følge af eksponenter synes måske i første omgang overflødigt, men gør det bekvemmere at formulere nogle af de følgende definitioner og sætninger. E15 Ø16

Berettigelsen af primspektret er følgende regneregler. Vi benytter $x \vee y$ for maximum og $x \wedge y$ for minimum. Vi benytter addition og subtraktion af følger, foretaget komponentvis. Vi benytter størrelsesrelationerne $<$ og $>$ og tilsvarende ved komponentvis sammenligning. Vi har altså at

$$(e^1, \ldots, e^i, \ldots) + (f^1, \ldots, f^i, \ldots) = (e^1 + f^1, \ldots, e^i + f^i, \ldots)$$
$$(e^1, \ldots, e^i, \ldots) < (f^1, \ldots, f^i, \ldots) \Leftrightarrow e^1 < f^1, \ldots, e^i < f^i, \ldots$$

20. Sætning: Regneregler for primspektret.

$$\sigma(ab) = \sigma(a) + \sigma(b)$$
$$a|b \Leftrightarrow \sigma(a) \leq \sigma(b)$$
$$a|b \Rightarrow \sigma(b/a) = \sigma(b) - \sigma(a)$$
$$\sigma(a \sqcap b) = \sigma(a) \wedge \sigma(b)$$
$$\sigma(a \sqcup b) = \sigma(a) \vee \sigma(b)$$

Bemærk at disse regler blot sammenfatter regler som er velkendte endda i folkeskolens matematik. En anvendelse har vi i

21. Sætning: Sammenhængen mellem sfd og mfm.

$$(a \sqcap b)(a \sqcup b) = ab$$

Bevis : *Sætningen bevises ved at vise at de to udtryk på hver side af lignhedstegnet har samme primspektrum, idet*

$$\sigma((a \sqcap b)(a \sqcup b)) = \sigma(a \sqcap b) + \sigma(a \sqcup b) = \sigma(a) \wedge \sigma(b) + \sigma(a) \vee \sigma(b)$$
$$\sigma(ab) = \sigma(a) + \sigma(b)$$

og idet det for alle x, y gælder at $(x \vee y) + (x \wedge y) = x + y$ (sum er sum af største og mindste !!) Ø17 Ø18

4: Modulær algebra.

Hvorfor egentlig modulær algebra?

I nogle sammenhænge er den interessante information i et tal dette tals rest ved division med et givet tal.

Her er et eksempel. Vi tænker os at vi benytter de hele tal til at angive tidspunkter det antal tidsenheder, fx timer, der er gået siden et givet begyndelsestidspunkt, med en passende konvention for anvendelse af negative tal. Men hvis vi kun er interesseret i hvilket tidspunkt på døgnet som svarer til dette tal, så er den interessante information knyttet til tallets rest ved division med antallet af tidsenheder på et døgn. Hvis der lige nu er gået 1024 timer fra begyndelsestidspunktet, og dette svarer til kl 0, da vil klokken nu være $1024 \bmod 24 = 16$. Hvis der er gået $31 \cdot 49$ timer vil vi nemt kunne regne ud at kl er 5 fordi vi kan se at klokken må være det samme som hvis der var gået $31(49 - 48) = 31$ timer. Vi skal i det følgende se på hvordan vi ud fra dette snusfornuftige ræsonnement kan systematisere regningen med rester.

Lad os tage endnu et eksempel, anvendelsen af 9-rester til beregningscheck: Ved 9-resten af et helt tal x forstås $x \bmod 9$. Netop 9-resten er nem at beregne: Start med at beregne tallets tværsum (summen af dets cifre), beregn tværsummens tværsum og fortsæt på denne måde indtil du har et enkelt ciffer, som så er 9-resten. Fx fås 9-resten af 27893 gennem følgende kæde af mellemregninger:

$27893 \to 29 \to 11 \to 2$. Hvis du skal finde 9-resten af produktet xy, skal vi komme til at se at dette gøres ved først at finde 9-resternen $x' = x \bmod 9$ og $y' = y \bmod 9$, beregne $x'y'$ og finde 9-resten af $x'y'$. Hvis da x og y er meget store og nogen påstår at $z = xy$, da kan du få et check af denne beregning ved at beregne 9-resten af xy som netop forklaret og sammenligne med 9-resten af z. Hvis man nemlig ikke kommer til samme resultat er der nemlig med garanti regnet forkert.

Den vigtigste anvendelse af regning med rester finder dog sted i forbindelsen med kryptering, men det vil vi først gå nærmere ind på, når vi har teorien på plads.

Historisk har regning med rester, modulær algebra, været knyttet til løsningen af store talteoretiske problemer, som fx Fermats sætning.

4.1: Baggrund for de modulære operationer

Definition af de modulære operationer.

Vi går lige på med det centrale hjul i maskineriet:

22. Sætning: Regning med restklasser

En sum og et produkt af restklasser er igen en restklasse:

$$[a_1]_b + [a_2]_b = [a_1 + a_2]_b, \quad [a_1]_b[a_2]_b = [a_1 a_2]_b$$

og vi kan beregne summen og produktet ved at regne med repræsentanter.

Bevis : *Lad $x \in [a_1]_b + [a_2]_b = (a_1 + b\mathbb{Z}) + (a_2 + b\mathbb{Z})$. Så findes $k_1, k_2 \in \mathbb{Z}$ så $x = (a_1 + bk_1) + (a_2 + bk_2) = (a_1 + a_2) + b(k_1 + k_2)$ og dermed at $x \in (a_1 + a_2) + b\mathbb{Z} = [a_1 + a_2]_b$. Derfor er $[a_1]_b + [a_2]_b \subseteq [a_1 + a_2]_b$.*

Den modsatte inklusion er en øvelse.

Lad $x \in [a_1]_b[a_2]_b = (a_1 + b\mathbb{Z})(a_2 + b\mathbb{Z})$. Så findes $k_1, k_2 \in \mathbb{Z}$ så $x = (a_1 + bk_1)(a_2 + bk_2) = (a_1 a_2) + b(a_2 k_1 + a_1 k_2 + k_1 k_2)$ og dermed at $x \in (a_1 a_2) + b\mathbb{Z} = [a_1 a_2]_b$. Derfor er $[a_1]_b[a_2]_b \subseteq [a_1 a_2]_b$.

Den modsatte inklusion er en øvelse.

Vi konstaterer ud fra formlerne, at hvis a_1 og a_2 er repræsentanter for klasser, da er $a_1 + a_2$ repræsentant for summen af de to klasser. Og analogt for produkt.

Det er altså meningsfuldt at tænke på hver restklasse som et enkelt objekt og på mængden af disse objekter udstyret med en addition og multiplikation. Vi kan understrege dette ved at lade hver klasse være karakteriseret ved en bestemt egenskab og regneoperationerne være defineret for disse egenskaber.

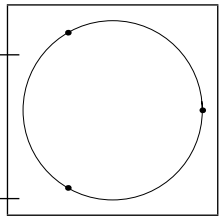
For $n = 2$ er der to klasser, hvor den ene består af de lige og den anden af de ulige tal. Her er det derfor oplagt at lade pariteten være den karakteriserende egenskab. Regning med klasser foregår da efter følgende regler:

$+$	*lige*	*ulige*
lige	*lige*	*ulige*
ulige	*ulige*	*lige*

$\times$	*lige*	*ulige*
lige	*lige*	*lige*
ulige	*lige*	*ulige*

For $n = 3$ er der tre klasser, med de tre repræsentanter -1,0 og 1. Lad os lade disse tre klasser være karakteriseret ved at repræsentere henholdsvis *tilbageskridt*,*stilstand* og *fremskridt*. Da vil addition af egenskaberne foregå efter reglerne i følgende skema:

$+$	*tilbageskridt*	*stilstand*	*fremskridt*
tilbageskridt	*fremskridt*	*tilbageskridt*	*stilstand*
stilstand	*tilbageskridt*	*stilstand*	*fremskridt*
fremskridt	*stilstand*	*stilstand*	*tilbageskridt*



Dette skema kan tillægges en mening hvis det fortolkes sammen med figuren til højre. Lad de tre karakteriseringer på naturlig måde svare til bevægelse mellem de fremhævede punkter på cirklen i overensstemmelse med deres ordlyd. Da svarer addition af to bevægelser til at lade bevægelserne følge efter hinanden.

Det er ikke tilsvarende oplagt at tillægge multiplikationen mening. Det gør nu ingen ting fordi vi i almindelighed har en meget effektiv karakterisering af hver klasse, nemlig dens principale rest modulo n. Det er (næsten) oplagt hvordan vi skal regne med de principale rester, selvom sum og produkt af principale rester ikke nødvendigvis selv er principale rester. Men det fremgår alt sammen af det følgende

4.2: Definition og egenskaber

23. Definition: Modulær algebra

Vi vil for ethvert $n > 0$ lade Z_n betegne mængden $\{x \in \mathbb{Z} : 0 \leq x < n\}$, altså mængden af principale rester modulo n. Vi indfører på $\mathbb{Z}_n$ følgende regneoperationer:

$$x \oplus y = (x + y) \bmod n$$
$$x \ominus y = (x - y) \bmod n$$
$$x \odot y = (xy) \bmod n$$
$$\ominus x = (-x) \bmod n$$

Vær opmærksom på at $\mathbb{Z}_n$ i andre sammenhænge som regel benyttes i en anden, men ækvivalent betydning. Mere herom senere.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Tabel 1. Additionstabel ($\oplus$) og multiplikationstabel ($\otimes$) i $\mathbb{Z}_4$)

Hvordan regner man modulært?

---

24. Definition: Algebraisk udtryk

Om et udtryk som er dannet ved gentagen brug af addition, subtraktion og multiplikation og elementer $a_1, \ldots, a_p$ fra $\mathbb{Z}$ vil vi sige at det er algebraisk frembragt af $a_1, \ldots, a_p$.

Analogt defineres et algebraisk udtryk i $\mathbb{Z}_n$

Eksempel : $2(a + b(3 + x)) + 2$ er algebraisk frembragt af $2, a, b, 3, x$.

Vi kan nu give en meget slagkraftig formulering af reglerne for regning med rester:

---

25. Definition: Principalreduktion

Lad u være et algebraisk udtryk frembragt af $a_1, \ldots, a_p$. Ved at erstatte hvert a_i med sin principale rest modulo n og erstatte hver operation med dens modpart i

$\mathbb{Z}_n$ fremkommer et algebraisk udtryk i $\mathbb{Z}_n$ som vi kalder den principale reduktion af u.

---

26. Sætning: Restdannelse respekterer algebraiske operationer.

Lad u være algebraisk frembragt af $a_1, \ldots, a_p$ og lad u' være den principale reduktion af u. Da vil u' være den pricipale rest af u.

Bevis : Lad os begynde med $u = a + b$. Vi skal da vise at $(a + b) \bmod n = (a \bmod n) \oplus (b \bmod n)$, altså at $(a+b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$. Men i følge ovenstående regel for regning med restklasser (S22), så har vi at $(a+b)$ og $(a \bmod n) + (b \bmod n)$ tilhører samme restklasse og derfor har samme principale rest. Samme argument kan anvendes på differenser og produkter. Og da ethvert algebraisk udtryk kan tænkes fremkommet ved successiv benyttelse af disse operationer enkeltvis fås sætningen. Vi illustrerer med følgende eksempel:

$(3 \cdot 5) + 5(4 \cdot 6) = 135$ og $135 \bmod 7 = 2$, mens $(3 \odot 5) \oplus 5 \odot (4 \odot 6) = 1 \oplus 5 \odot 3 = 1 \oplus 1 = 2$.

Vi reformulerer lige et par af de tidligere eksempler:

$(31 \cdot 49) \bmod 24 = (31 \bmod 24) \odot (49 \bmod 24) = 7 \odot 1 = 7$.

$(xy) \bmod 9 = (x \bmod 9) \odot (y \bmod 9)$.

og et nyt eksempel:

Beregn $5^{117} \bmod 7$. Vi benytter $a \equiv b$ til at notere at a og b har samme principale rest modulo 7.

Først beregnes en række potenser successivt:

$5^2 \equiv 4$, $5^4 \equiv 4^2 \equiv 2$, $5^8 \equiv 4$, $5^{16} \equiv 2$, $5^{32} \equiv 4$,$5^{64} \equiv 2$.

Da $117 = 64 + 32 + 16 + 4 + 1$ fås da at $5^{117} \equiv 5^{64}5^{32}5^{16}5^{4}5^{1} \equiv 2 \cdot 4 \cdot 2 \cdot 2 \cdot 5 \equiv 16 \cdot 10 \equiv 2 \cdot 3 = 6$

Bemærk at

$$5^{117} = 60185310762101120407999310705778978704315676506730881101248087361454963684082031 25$$

En systematisk fremgangsmåde er følgende:

27. Sætning: De modulære operationer har de forventede pæne egenskaber.

De modulære operationer opfylder de sædvanlige algebraiske regneregler. Sum og produkt er kommutative og associative, subtraktion er det modsatte af addition og multiplikation er distributiv mht addition.

Bevis : Vi tager distributiviteten som et eksempel: $a \odot (b \oplus c) = (a(b+c)) \bmod n = (ab + ac) \bmod n = a \odot b \oplus a \odot d$. *Resten er en øvelse,* `'xrsModulRegler'`

Vi slutter af med at se på, hvordan og hvornår man kan dividere. Dette begrunder et par nye begreber.

4.3: Modulær division

Modulære enheder og Eulers funktion

---

28. Definition: Reciprok.

Lad $a, b \in \mathbb{Z}_n$. *Vi siger at* b *er reciprok til* a *modulo* n, *hvis* $a \otimes b = 1$. *Vi siger at* a *er multiplikativt invertibel hvis* a *har en reciprok*

---

29. Sætning: Modulær reciprok.

Lad $a \in \mathbb{Z}$. *Da har* a *en reciprok netop hvis* a *og* n *er indbyrdes primiske.*

Bevis : Antag at a *og* n *er indbyrdes primiske. Vi har at* $a \sqcap n = 1$. *Vi kan derfor finde* $x, y \in \mathbb{Z}$ *således at* $xa + yn = 1$. *Sæt* $b = x \bmod n$. *Vi kan da finde* $q \in \mathbb{Z}$ *så at* $x = b + qn$. *Vi får da at* $1 = xa + yn = ab + aqn + yn = ab + (aq + y)n$ *og derfor vil* $ab \bmod n = 1$ *og det er det samme som at* $a \otimes b = 1$, *så* b *er altså reciprok til* a.

Antag så at a *har en reciprok* b, *altså at* $ab \bmod n = 1$. *da er* ab *og* n *indbyrdes primiske. Altså må der findes* p *og* q *således at* $pab + qn = 1$. *Heraf følger at* $a \sqcap n$, *som jo både går op i* a *og* n *også må gå op i* 1. *Det kan ikke ske uden at* $a \sqcap n = 1$. *Derfor er altså* a *og* n *indbyrdes primiske.*

---

30. Definition: Modulær reciprok.

Det i sætningen nævnte a' *kaldes for det reciprokke element af* a *modulo* n, *og betegnes* a^{-1}

Eksempel: Da $33 \sqcap 65 = 1 = 2 \cdot 33 + (-1) \cdot 65$ har vi at 2 er reciprok til 33 modulo 65. Ø19

31. Sætning: Modulær division.

Lad $a \in \mathbb{Z}_n$ være invertibel modulo n, og lad $b \in \mathbb{Z}_n$. Da findes netop et element $x \in \mathbb{Z}_n$ således at $a \otimes x = b$.

Bevis : *Sæt $x = a^{-1}b$. Da er $ax = aa^{-1}b = b$.*

32. Sætning: Eksistens af endelige legemer.

Hvis n er et primtal da har enhver ligning af formen $a \otimes x = b$, hvor $a \neq 0$ netop en løsning. Dette betyder at $\mathbb{Z}_n$ et legeme.

Bevis : *Hvis n er et primtal, da er ethvert element $x \in \mathbb{Z} - n$ indbyrdes primisk med n, bortset fra $x = 0$. Heraf ses at enhver ligning af formen $ax = b$ med $a \neq 0$ har netop en løsning.*

4.4: Eulers ϕ-funktion.

33. Definition: Enhedsgruppen, Eulers ϕ

Vi siger at x er en enhed modulo n, hvis x er invertibel modulo n. Det er en lidt forvirrende betegnelse som bedre kan forklares i en større sammenhæng, hvilket vi så undlader. Vi kalder mængden af enheder modulo n for enhedsgruppen modulo n og betegner den $\Phi(n)$. Vi betegner antallet af enheder modulo n med $\varphi(n)$. Med denne definition er $\varphi(1)$ ikke defineret, men det viser sig bekvemt at udvide definitionen med $\phi(1) = 1$. Funktionen $\varphi : \mathbb{N} \to \mathbb{N}$ defineret på denne måde kaldes for Eulers funktion, Eulers φ-funktion eller Eulers totientfunktion. Den spiller en meget vigtig rolle i talteorien.

Vi vil nøjes med et enkelt resultat, en formel som gør det muligt at beregne funktionsværdierne rekursivt, idet $\varphi(n)$ er kædet sammen med funktionsværdierne for divisorerne i n.

34. Sætning: En fundamental formel for φ.

$$\sum_{d|n} \phi(d) = n$$

Bevis : *Vi sætter*

$$N = \{x : 1 \leq x < n\}$$

og for hver $d > 1$ *for hvilket* $d|n$ *sætter vi*

$$G_d = \{x \in N : x \sqcap n = d'\},$$

hvor vi har defineret $d' = \frac{n}{d}$. *Det er da oplagt at* N *er disjunkt forening af disse* G_d, *som jo er "niveaumængderne" for funktionen* $x \mapsto x \sqcap n$. *F.eks. fås for* $n = 12$ *og* $d = 3$ *at* $d' = 4$ *og at* $G_3 = \{4, 8\}$. *Se i øvrigt udregningerne efter beviset.*

Vi vil vise at G_d *har* $\varphi(d)$ *elementer. Vi har per definition at* $x \sqcap n = d'$ *hvis* $x \in G_d$, *og ved at dividere på begge sider af denne ligning med* d' *fås at* $\frac{x}{d'} \sqcap d = 1$. *Desuden gælder oplagt at* $\frac{x}{d'} < d$. *Alt i alt har vi så at* $\frac{x}{d'} \in \Phi(d)$.

Definerer vi nu afbildningen $F : G_d \to \mathbb{Z}$ *ved at sætte* $F(x) = \frac{x}{d'}$, *da har vi altså vist at* $F(x) \in \Phi(d)$.

F *er oplagt injektiv.*

Vi vil også vise at F *er surjektiv, altså at* $F(G_d) = \Phi(d)$. *Lad nemlig* $y \in \Phi(d)$. *Ved multiplikation på begge sider af* $y \sqcap d = 1$ *med* d', *fås at* $yd' \sqcap n = d'$ *og da* $y < d$ *så vil* $yd' < n$. *Vi har derfor at* $yd' \in G_d$. *Da* $F(yd') = y$ *har vi altså at* $F(G_d) = \Phi(d)$.

I eksemplet er $F(x) = \frac{x}{4}$ *og* $F(G_3) = \{1, 2\} = \Phi(3)$.

Alt i alt har vi altså at F *er en bijektion af* G_d *på* $\Phi(d)$. *Dette betyder at* G_d *indeholder* $\phi(d)$ *elementer. I alt vil* N *indeholde* $n - 1$ *elementer. Ved at udnytte at antallet af elementer i* N *må være summen af antallet af elementer i* G_d, *når* $d > 1$ *gennemløber divisorerne i* n *fås*

$$\sum_{d|n, d>1} \phi(d) = n - 1.$$

Ved i denne formel at addere $\varphi(1) = 1$ på begge sider fås den postulerede formel.

Beviset er illustreret for $n = 12$ i følgende skema, som det er meget illustrativt at gennemgå

	d	d'	G_d	$\Phi(d)$	$\varphi(d)$
1	1	12	$\{12\}$	$\{1\}$	1
2	2	6	$\{6\}$	$\{1\}$	1
3	3	4	$\{4, 8\}$	$\{1, 2\}$	2
4	4	3	$\{3, 9\}$	$\{1, 3\}$	2
5	6	2	$\{2, 10\}$	$\{1, 5\}$	2
6	12	1	$\{1, 5, 7, 11\}$	$\{1, 5, 7, 11\}$	4

Ø20 E21

Til brug i næste afsnint om kryptering tager vi også lige

35. Sætning: Fermats lille sætning

Lad p være et primtal og lad a og p være indbyrdes primiske. Da er $a^{p-1} \bmod p = 1$.

Bevis : For elementer af $\mathbb{Z}_p$ vil vi lade det fremgå af sammenhængen om operationerne skal forstås som de sædvanlige eller de modulære.

Vi sætter $b = a \bmod p$, da er $a^{p-1} \bmod p = b^{p-1}$. Da a og p er indbyrdes primiske vil b være et invertibelt element i $\mathbb{Z}_p$. Afbildningen $\mathbb{Z}_p \ni x \mapsto bx \in \mathbb{Z}_p$ er derfor en bijektion. Vi har altså at $\{bx : x \in \mathbb{Z}^p\} = \mathbb{Z}_p$ og derfor er

$$= (1 \cdots (p-1)) = (1 \cdot b) \cdots ((p-1) \cdot b) = (1 \cdots (p-1))b^{p-1}.$$

Det første lighedstegn begrundes af at der på hver side er et produkt med de samme faktorer (men i forskellig rækkefølge). Det andet ved simple regneregler. Af den resulterende ligning mellem de yderste udtryk fås ved forkortning at $b^{p-1} = 1$, som postuleret i sætningen.

Kryptering.

Lad p og q være primtal; sæt $n = pq$. Vha Eulers formel fås at

$$\varphi(n) = n - \varphi(p) - \varphi(q) - \varphi(1) = pq - (p-1) - (q-1) - 1 = (p-1)(q-1).$$

Lad $c \in \mathbb{Z}_{\varphi(n)}$ være invertibel og sæt $d = c^{-1}$. Vi har da at der findes r således at $cd = 1 + \varphi(n)r$.

Vi definerer for $x < n$ funktionerne F og G ved $F(x) = x^c \bmod n$ og $G(x) = x^d \bmod n$. Vi vil vise at de er hinandens inverse. Vi ser at $G(F(x)) = x^{cd} \bmod n = x^{1+\varphi(n)r} \bmod n = x(x^{(p-1)(q-1)})^r = x(x^{p-1})^{(q-1)r}$. Hvis nu x og p er indbyrdes primiske, da er $x^{p-1} = 1$ ifølge S 35. Så i dette tilfælde er $F(G(x)) = x$. Ellers vil x og q være indbyrdes primiske og et symmetrisk argument med p og q ombyttet giver da at formlen også gælder i dette tilfælde.

Derfor er G den inverse af F.

Dette benyttes i kryptering på følgende måde: Du oplyser helt offentligt at folk der vil sende dig noget krypteret blot skal bruge F som krypteringsfunktion. Du skal oplyse n og c, som kaldes din offentlige nøgle. Du kan da dekryptere ved at benytte G, hvilket du jo kan fordi du kender d, som du ikke må oplyse andre om.

Pointen i dette er at det er meget vanskeligt for andre at finde dekrypteringsfunktionen, altså finde d, selvom d jo er entydigt fastlagt ud fra de kendte størrelser. Hvis n indeholder mange hundrede cifre er det umuligt at bestemme $\phi(n)$ selv ved brug af formlen ovenfor. Verdens for øjeblikket hurtigste computer kan ikke gøre det inden for universets levetid. Hvis man kunne finde primfaktoropspaltningen $n = pq$ ville det ikke være nogen sag. Men primfaktorisering af meget store tal hører til de mest tidskrævende opgaver. Man har dog ikke kunnet bevise at der ikke findes en smart effektiv metode til primtalsfaktorisering.

Der findes meget tilgængelig literatur om denne krypteringsmetode.

5: Epilog

Der har været to hovedtemaer:

1) samspillet mellem to primære binære operationer, addition og multiplikation, i forskellige sammenhænge.
2) overførsel af en struktur af denne type fra en mængde til en anden ved hjælp af en ækvivalensrelation. Ækvivalensklasserne bliver de nye objekter og addition og multiplikation overføres hertil.

At overføre de primære operationer addition og multiplikation går ganske let. Når vi vil undersøge muligheden for at overføre division må der imidlertid inddrages raffinerede om end velprøvede redskaber nemlig den enkle og den udvidede euklidiske algoritme.

Disse metoder har interesse i sig selv og indgår derudover også væsentligt i nogle af de algebraiske sidetemaer:

1) primtalsfaktorisering af hele tal
2) metoder til bestemmelse af største fælles divisor og mindste fælles mangefold

De nævnte metoder til bestemmelse af største fælle divisor illustrerer et alment algebraisk tema, nemlig det at overføre en opgave i et univers (her de naturlige tal med største fælles divisor som operation) til et andet univers (her bestående af visse følger af hele tal med komponentvis minimum som operation).

Overførslen sker ved hjælp af primspektret, en afbildning som til et naturligt tal knytter en vis følge, en afbildning som har en logaritmeagtig virkning.

Denne kan også bruges til at transformer produktoperationen til komponentvis addition af de omtalte følger.

Det sammenfattes i regneregler for denne transformation som minder om regneregler for logaritmer og er eksempler på det der i abstrakt algebra kaldes homomorfier.

6: Eksempler og øvelser

Øvelse 1: Lav beviset
Bevis S1

Eksempel 2: Delelighed
$3|12, -3|12, 3|(-12), 0|0, 7|0$.

Øvelse 3: Divisorer
Bestem mængden af divisorer i $-25{,}35$ og 0.

Eksempel 4: Bestemmelse af største fælles divisor
$15 \sqcap 12 = 3, (-35) \sqcap 14 = 7, 0 \sqcap (-12) = 12, \bigsqcap 3\mathbb{Z} = 3$. Og $15 \sqcup 25 = 75$, $12 \sqcup 18 = 36$.

Øvelse 5: Find største fælles divisor
Bestem $39 \sqcap 52$ og $48 \sqcap 36 \sqcap 18$.

Øvelse 6: Lav beviset
Bevis S2

Eksempel 7: Bestemmelse af rest
Vi har at 7 er en rest af 19 modulo 4, da $19 = 3 \cdot 4 + 7$ og at $[5]_4 = \{\ldots, -7, -3, 1, 5, 9 \ldots\}$.

Øvelse 8: Bestemmelse af rest
Bestem tre forskellige rester af 25 modulo 4.

Eksempel 9: Bestemmelse af principal rest
$8 \bmod 6 = 2, (-8) \bmod 6 = 4$.

Øvelse 10: Bestemmelse af principal rest
Bestem den principale rest af -31 modulo 5.

Øvelse 11: Symmetrisk rest
Man kan også som særlig rest vælge den rest, som er nummerisk mindst. Den kaldes den symmetriske rest. Se på nogle eksempler og overvej om definitionen er skarp nok.

Øvelse 12: Beregning af plads i geledet
Antag at en række rekrutter er stillet op på en lang række og nu skal ordnes ind på række og geled ved at udfylde rækkerne først. Hvis der er n geledder

vil rekrut nr i skulle stå i række nr i div n og geled nr $i \bmod n$. Vel at mærke hvis vi nummererer fra 0. Hvad bliver resultatet hvis vi nummerer fra 1?

Øvelse 13: Benyttelse af Euklids algoritme
Beregn $231 \sqcap 375$

Øvelse 14: Anvendelse af den udvidede algoritme.
Bestem $x, y \in \mathbb{Z}$ så at $231 \sqcap 375 = x231 + y375$.

Eksempel 15: Bestemmelse af primspektrum
$\sigma(12) = (2, 1)$, $\sigma(63) = (0, 2, 0, 1)$, idet vi undlader at skrive de sidste (mange) nuller.

Øvelse 16: Intelligensprøve
Find næste led: $0, 1, 01, 2, 001, 11, 0001, 3$

Øvelse 17: Analogi med logaritmer
Gør rede for at nogle af regnereglerne for primspektret svarer til regneregler for logaritmer, og overvej hvorfor der er denne analogi.

Øvelse 18: Øv dig i brug af regnereglerne
Bestem $(a \sqcap b)$ og $(a \sqcup b)$ for følgende par (a, b):

$(2^4 \cdot 5^3 \cdot 11^2, 2^2 \cdot 3 \cdot 11^3 \cdot 79), (242000, 1261788), (2205, 189)$

Øvelse 19: Bestemmelse af modulær reciprok
Bestem 3^{-1} i $\mathbb{Z}_{65}$.

Øvelse 20: Lav dit eget skema
Lav et tilsvarende skema for et eller flere af tallene $n = 15, 18, 21$

Eksempel 21: Beregning af φ vha Eulers formel
Lad os beregne $\varphi(72)$.

Vi noterer at de ægte divisorer i 72 er $1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36$.

Det er nemt ud fra definitionen at vise at

$$\varphi(2) = 1, \quad \varphi(3) = 2, \quad \varphi(4) = 2, \quad \varphi(6) = 2,$$

og ud fra disse værdier kan vi beregne

$$
\begin{aligned}
\varphi(8) &= 8 - \varphi(4) - \varphi(2) - \varphi(1) = 8 - 2 - 1 - 1 = 4 \\
\varphi(9) &= 9 - \varphi(3) - \varphi(1) = 9 - 2 - 1 = 6 \\
\varphi(12) &= 12 - \varphi(6) - \varphi(4) - \varphi(3) - \varphi(2) - \varphi(1) = 12 - 2 - 2 - -21 - 1 = 4 \\
\varphi(18) &= 18 - \varphi(9) - \varphi(6) - \varphi(3) - \varphi(2) - \varphi(1) = 18 - 6 - 2 - 1 - 1 = 8 \\
\varphi(24) &= 24 - \varphi(12) - \varphi(8) - \varphi(6) - \varphi(3) - \varphi(2) - \varphi(1) \\
&= 24 - 4 - 4 - 2 - 2 - 2 - 1 - 1 = 8 \\
\varphi(36) &= 36 - \varphi(18) - \varphi(12) - \varphi(9) - \varphi(6) - \varphi(3) - \varphi(2) - \varphi(1) \\
&= 36 - 8 - 6 - 6 - 2 - 2 - 1 - 1 = 12 \\
\varphi(72) &= 72 - \varphi(36) - \varphi(24) - \varphi(18) - \varphi(12) - \varphi(9) - \varphi(6) - \varphi(3) - \varphi(2) - \varphi(1) \\
&= 72 - 12 - 8 - 8 - 6 - 6 - 2 - 2 - 1 - 1 = 24
\end{aligned}
$$

Anders Madsen

LEGEMER OG VEKTORRUM

KONKRETE ALGEBRAISKE STRUKTURER

5

Indholdsfortegnelse

1: Prolog

I dette hæfte skal du møde forskellige konkrete eksempler på algebraiske strukturer. Vi taler om en algebraisk struktur, når vi har en bestemt type objekter og en eller flere operationer på denne type objekter, der fører til et objekt af samme type, samt nogle regneregler for disse operationer.

Det mest oplagte eksempel har som objekter de reelle tal, som operationer de sædvanlige aritmetiske operationer med de sædvanlige regneregler.

Hæftet handler om legemer og vektorrum over legemer. Der er i grove træk tale om et resume af sådanne begreber og resultater fra de reelle tals legeme og vektorrum over de reelle tal, som umiddelbart også gælder for vilkårlige legemer. At resultaterne kan overføres med enslydende beviser — mutatis mutandis — postuleres, men gennemføres ikke i detaljer. Det er tænkt som udgangspunkt for en perspektiverende genlæsning af teorien for reelle vektorrum.

Legemer defineres helt abstrakt og der gives en del konkrete eksempler, herunder visse endelige legemer, nemlig dem hvis orden er et primtal. De endelige legemer præsenteres som konkrete mængder med konkret operationer uden bevis for at de opfylder aksiomerne for legemer. Det vil derfor være kærkomment hvis læseren i forvejen har stiftet bekendtskab med restklasseringen af de hele tal modulo et primtal. Men det er meningen at man skal kunne læse og forstå teksten her, blot man er indstillet på at acceptere postulaterne.

Hovedformålet er at vise hvordan man kan regne i alle legemer på samme måde som i mønsterlegemet de reelle tal med visse ekstra regneregler afhængigt af legemet. Dette er fremhævet ved at resumere hvilke resultater der for de reelle tal gælder for behandling af lineære ligningssystemer, herunder anvendelse af matricer og postulere at disse resultater også gælder for vilkårlige legemer.

Vektorrum over et vilkårligt legeme defineres. Definitioner og sætninger fra de reelle tals tilfælde opsumeres. Enkelte beviser gives. Der vil være en opsamling med tydeligørelse af den røde tråd i epilogen.

2: Legemer

2.1: Definition

1. Definition: Legeme

Et legeme er en mængde L udstyret med fire regneoperationer $+, -, \cdot, :$ og hvor der er udpeget to elementer 0 og 1 således at

1) $a+b, a-b, ab$ *er defineret for alle* a, b
2) $a : b$ *er defineret for alle* a *og* b*, blot* $b \neq 0$
3) $a+b = b+a$ *og* $ab = ba$ *for alle* a, b
4) $a+(b+c) = (a+b)+c$ *og* $a(bc) = (ab)c$ *for alle* a, b, c
5) $a(b+c) = ab+ac$ *for alle* a, b, c
6) $a+0 = a$ *og* $a1 = a$ *for alle* a
7) *Ligningen* $a+x = b$ *i den ubekendte* x *har netop en løsning, nemlig* $x = b-a$*, for alle* a, b.
8) *Ligningen* $ax = b$ *i den ubekendte* x *har netop en løsning, nemlig* $x = b : a$*, for alle* a *og* b*, blot* $a \neq 0$.

---

2. Sætning: De sædvanlige legemer

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ *er legemer når* $+, -, \cdot, :, 0, 1$ *har den sædvanlige betydning.*

E1 Ø2 Ø3

2.2: Nogle endelige legemer

3. Sætning: Lemma

Lad p være et primtal. Antag at de naturlige tal a, b opfylder $0 \leq a < p$ og $0 < b < p$. Da har ligningen $(bx) \bmod p = a$ netop en løsning x som opfylder $0 \leq x < p$.

Bevis : beviset (som er meget smukt) gives ikke her. Men vi kan illustrere og dokumentere indholdet af sætningen ved at se på følgende tabel over $(bx) \bmod p$, hvor $p = 5$:

	0	*1*	*2*	*3*	*4*
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

I hver række er anført produkterne $(bx) \bmod 5$ for et fast b. Vi ser at ethvert a med $0 \leq a < p$ forekommer i denne række. Det betyder at der til ethvert a

findes x så $bx = a$. Og da hvert a forekommer netop en gang er der altså en entydig løsning til $bx = a$.

4. Sætning: Endelige legemer.

Lad p være et primtal. Sæt $L = \{x \in \mathbb{Z} : 0 \leq x < p\} = \{0, 1, \ldots, p-1\}$. Definer følgende operationer

$a \oplus b = (a + b) \bmod p$

$a \ominus b = (a - b) \bmod p$

$a \odot b = (ab) \bmod p$

$a \oslash b$ *er løsningen til* $bx = a \pmod{p}$

Med disse operationer (og oplagt 0 *og* 1*) udgør L et legeme.*

5. Definition: $\mathbb{Z}_p$

Det i foregående sætning nævnte legeme benævnes $\mathbb{Z}_p$

I det følgende benyttes de sædvanlige operationstegn og ikke de omringede. Det er kun naturligt hvis det kan give lidt problemer i startenSystemer af lineære ligninger med reelle koefficienter og reelle ubekendte er formuleret udelukkende ved brug af de fire regneoperationer. Dette gælder også de sædvanlige løsningmetoder vha Gaussisk elimination og deres gyldighed beror udelukkende på regnereglerne for legemer.

Derfor er det oplagt at betragte de definitioner og metoder som fremstår når de reelle tal erstattes med et vilkårligt legeme. Dette udstrækkes også til brugen af matricer med elementer taget fra legemet. Dette er illustreret i følgende eksempler og øvelser: E4 Ø5 Ø6 Ø7 E8

Vi har nu set eksempler på endelige legemer, hvor antallet af elementer er et primtal. Der findes faktisk flere. Vi kan ikke her gå ind på hvordan de konstrueres, men kan dog tage et enkelt eksempel på et legeme med 4 elementer. E9

3: Vektorrum over vilkårligt legeme

3.1: Definition af de fundamentale begreber

Det følgende er skrevet i forventning om at læseren er bekendt med vektorrum over de reelle tal, altså vektorrum hvor man kan danne skalarproduktet af et reelt tal og en vektor. I den følgende definition indgår et legeme L og læseren forventes derfor at genkende følgende definition i det tilfælde hvor L er de reelle tals legeme.

6. Definition: Vektorrum over vilkårligt legeme

Lad V være en mængde og L et legeme. Vi siger at V er et vektorrum over L, hvis der findes operationer $+, -, \cdot$ og et udpeget element 0 i V, således at

1) $u + v, u - v$ er defineret for alle $u, v \in V$
2) au er defineret for alle $u \in V$ og alle $a \in L$
3) $u + v = v + u$ for alle $u, v \in V$
4) $u + 0 = 0$ for alle $u \in V$
5) $a(u + v) = au + av$ og $(a + b)u = au + bu$ for alle $a, b \in L, u, v \in V$
6) $a(bu) = (ab)u$ for alle $a, b \in L, u \in V$
7) Ligningen $u + x = v$ i den ubekendte x har netop en løsning, nemlig $x = v - u$ for ethvert $u, v \in V$

Elementerne i V kaldes vektorer og elementerne i L kaldes skalarer.

Følgende definitioner fra reelle vektorrum er formuleret alene vha addition og skalarmultiplikation og kan derfor anvendes i den samme formulering også i den generelle situation:

Idet $A, B \subset V$, $v, v_1, \ldots, v_k \in V$, $a, a_1, \ldots, a_n \in L$ har vi defineret hvad det vil sige at

1) v er linearkombination af $v_1, \ldots, v_k$ med koefficientsæt $(a_1, \ldots, a_k)$
2) A er det lineære hylster af B (eller B udspænder A), skrevet $A = \text{span}B$
3) A er et underrum af V
4) A er lineært uafhængig
5) A er en basis for B
6) A har dimensionen n

Det kan med oplagte modifikationer af beviserne ses at følgende resultater også gælder for generelle legemer:

7) span$A$, er et underrum

Idet V og W er vektorrum over det samme legeme L, T er en afbildning af V ind i W, $A \subset V$, $B \subset W$, har vi defineret hvad det vil sige at

8) T er lineær
9) T er en isomorfi
10) A er nulrummet (eller kernen) for T, skrevet $A = \mathcal{N}(T)$.
11) B er billedrummet (engelsk range) for T, skrevet $B = \mathcal{R}(T)$

og det gælder at

12) $\mathcal{N}(T)$,$\mathcal{R}(T)$ er underrum
13) sammensætning, invers og sum af lineærere afbildninger er lineær

Standardeksemplet på et vektorrum over L er $V = L^n$ og standardeksemplet på en lineær afbildning er en afbildning T af formen $T(x) = Ax$, hvor A er en $m \times n$ matrix. Enhver lineær afbildning af L^n ind i L^m vil være af denne form, hvor matricen er bestemt ved at $A^i = T(e^i)$. Vi noterer sammenhængen mellem T og A ved at skrive $T = \widehat{A}$. Denne sammenhæng mellem lineære afbildninger og matricer gør det muligt at flytte regninger med lineære afbildninger over til regning med matricer i kraft af følgende regler

14) $\widehat{A_1 A_2} = \widehat{A_1} \circ \widehat{A_2}$
15) $\widehat{A_1 + A_2} = \widehat{A_1} + \widehat{A_2}$
16) $\widehat{aA_1} = a\widehat{A}$

For endeligdimensionale vektorrum kan man bruge talrummene L^n som model og derved flytte opgaver der er formuleret i et vektorrum over til overgaver i et talrum. Dette beror på følgende:

Til $\mathcal{V} = (v_1, \ldots, v_n)$, knytter vi afbildningen $I_\mathcal{V} : L^n \to V$ givet ved $I(x_1, \ldots, x_n) = x_1 v_1 + \ldots + x_n v_n$ da gælder at

17) $I_\mathcal{V}$ er lineær
18) $\{v_1, \ldots, v_n\}$ er lineært uafhængig hvis og kun hvis $I_\mathcal{V}$ er injektiv
19) $\{v_1, \ldots, v_n\}$ udspænder V hvis og kun hvis $I_\mathcal{V}$ er surjektiv
20) $\{v_1, \ldots, v_n\}$ er en basis for V hvis og kun hvis $I_\mathcal{V}$ er bijektiv. I så fald kaldes den omvendte afbildning $K_\mathcal{V}$ for koordinatafbildningen med hensyn til $\mathcal{V}$ og vi noterer billedet af $v \in B$ med $K_\mathcal{V}(v) = [v]_\mathcal{V}$

Hvis vektorerne i $\mathcal{V} = (v_1, \ldots, v_n)$ udgør en basis for V og vektorerne i $\mathcal{W} = (w_1, \ldots, w_m)$ udgør en basis for W da findes en $m \times n$ matrix A over L således

at det for alle $v \in V$ gælder at

$$[T(v)]_{\mathcal{W}} = A[v]_{\mathcal{V}}, \quad (K_{\mathcal{W}} \circ T = \widehat{A} \circ K_{\mathcal{V}}),$$

specielt gælder at $[T(v_i)]_{\mathcal{W}} = Ae^i = A^i$, dvs søjle nr i i A er koordinatsættet for $T(v_i)$ mht $\mathcal{W}$. Matricen A betegnes med $[T]^{\mathcal{V}}_{\mathcal{W}}$.

En række forskellige vektorrum er illustreret i følgende eksempler og øvelser:

Ø10 E11 Ø12

3.2: Den kanoniske bilinearform, pseudoortogonal

Et vigtigt redskab for reelle vektorrum er indre produkt, fordi det indgår i formuleringen af de "geometriske" begreber som afstand, ortogonalitet og (ortogonal) projektion, som igen benyttes i optimering som fx mindste kvadraters metode.

Dette værktøj kan vi ikke kopiere til generelle legemer. Det kan generaliseres til de komplekse tal, men det vil vi ikke komme ind på her.

Her ønsker vi nemlig at se på generelle legemer. Dog nøjes vi med endelig dimensionale vektorrum, endda kun i modelformen Ł^n.

Definitionen af det indre produkt i $\mathbb{R}^n$ kan sagtens kopieres, og nogle af de samme simple sammenhænge, gælder stadig:

$$x \cdot y = x_1 y_1 + \ldots + x_n y_n = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = x^\top y$$

Men dette prikprodukt vil ikke i almindelighed være et indre produkt. Kravet om at $x \cdot x \geq 0$ har som regel slet ikke mening fordi der ikke er en naturlig ordningsrelation i L.

Grunden til at det alligevel kan være nyttigt er at det spiller sammen med matrixmultiplikation. Hvis vektorer automatisk identificeres med søjlevektorer, dvs $n \times 1$ matricer, vil vi jo have at

$$x \cdot y = x^\top y, \text{ og } C_{ij} = A_i \cdot B^j,$$

hvor A, B, og C er matricer med $C = AB$ og A_i er række nr i i A, B^j er søjle nr j i B, opfattet som vektorer.

Betingelsen $x \cdot y = 0$, som i det reelle tilfælde definerer ortogonalitet, har dog mening generelt og kan benyttes til formulering af visse resultater om nulrum og billedrum, som vi kender fra det reelle tilfælde.

7. Sætning: Pseudo indre produkt.

Lad L være et legeme og lad $V = L^n$. Da defineres der ved

$$x \cdot y = x_1 y_1 + \ldots x_n y_n$$

en operation som vi vil kalde det pseudo indre produkt på V. Dette indre produkt er bilineært. Vi

8. Definition: Pseudoortogonal

Vi siger at x og y er pseudoortogonale hvis $x \cdot y = 0$ og skriver dette $x \perp y$. Nogle forfattere siger at x og y er indbyrdes polære.

Vi definerer det pseudoortogonale underrum $A^\perp$ for en delmængde A som mængden af vektorer som er vinkelrette på enhver vektor i A.

(Denne mængde kaldes også polaren for A og betegnes også A°.)

9. Sætning: Regneregler for pseudoortogonalitet

$$A \subset A^{\perp\perp}, \quad \mathcal{N}(A)^\perp = \mathcal{R}(A^\top), \quad \mathcal{R}(A)^\perp = \mathcal{N}(A^\top)$$

I endeligdimensionale vektorrum over $\mathbb{R}$ betegnes $A^\perp$ som det ortogonale komplement, fordi det er et underrum og sammen med A spalter hele vektorrummet i en direkte sum.

Sådan forholder det sig slet ikke ved pseudoortogonalitet, så betegnelsen komplement ville ikke være velvalgt. Du kan se et eksempel i E13 E14 E15 Ø16

Vektorrum over endelige legemer spiller en meget stor rolle i moderne matematik, hvor de er helt essentielle i kodningsteori, læren om hvordan man sender meddelelser uden at de forstyrres af støj, altså således at det er mulig at rekonstruere en meddelelse selv om noget af dens indhold er gået. De spiller også en stor rolle i tilrettelæggelse af strategier som hviler på kombinatorik.

3.3: Spektralanalyse

Lad os resumere definitioner og notation.

10. Definition: Spektrum

Lad V være et vektorrum over L og lad T være en lineær afbildning af V ind i V. Lad $\lambda \in L$.

1) *Vi sætter* $E(\lambda) = \{v \in V : T(v) = \lambda v\}$
2) *Vi sætter* $\text{geo}(\lambda) = \dim(E(\lambda))$
3) *Vi sætter* $\sigma(T) = \{\lambda : \text{geo}(\lambda) > 0\}$
4) *Vi kalder $\sigma(T)$ for spektret for T*

Hvis $\lambda \in \sigma(T)$ siger vi at

5) *λ er en egenværdi for T*
6) *$E(\lambda)$ er egenrummet hørende til λ*
7) *v er en egenvektor hørende til λ hvis $v \in E(\lambda)$ og $v \neq 0$*
8) $\text{geo}(\lambda)$ *er den geometriske multiplicitet af λ*

Hvis $V = L^n$ og A er den matrix for hvilken $T = \widehat{A}$, da benytter vi ovenstående definitioner med T erstattet af A. Vi har da også følgende betegnelser

9) *For $x \in L$ sættes* $\chi_A(x) = \det(A - xE)$
10) *Vi kalder χ_A for det karakteristiske polynomium for A*
11) $\text{alg}(\lambda)$ *er rodmultipliciteten af λ som rod i χ_A, dvs det største tal r for hvilket $(x - \lambda)^r$ er faktor i χ_A*
12) *Vi kalder* $\text{alg}(\lambda)$ *for den algebraiske multiplicitet for λ.*

---

og vi har da følgende hovedkriterium for egenværdier TheoremMtheKarakteristiskSpektret består af nulpunkterne for det karakteristiske polynomium spektret for A består af nulpunkterne for det karakteristiske polynomium

11. Definition: Diagonaliserbar matrix

Vi siger at T er diagonaliserbar hvis der en diagonalmatrix D således at $T = \widehat{D}$. Vi siger at A er diagonaliserbar hvis $\widehat{A}$ er diagonaliserbar

---

TheoremMtheDiagonaliserbarhedKriterier for diagonaliserbarhedMatricen A er diagonaliserbar netop hvis et af følgende kriterier er opfyldt

1) Der findes en basis af egenvektorer for A

2) Der findes en invertibel matrix S og en diagonalmatrix D således at $D = S^{-1}AS$
3) Der findes en invertibel matrix S og en diagonalmatrix D således at $SD = AS$
4) Der findes en invertibel matrix S hvis søjler er egenvektorer således at $SD = AS$ hvor D er en diagonalmatrix hvis diagonalelementer er egenværdier, idet S^i svarer til D_{ii}

Bevis : (1) medfører (2): Lad T være $\widehat{A}$. I basen bestående af egenvektorer vil T have en diagonalmatrix D. Da D og A er matricer for samme afbildning T vil disse to matricer være similære, hvilket per definition er indholdet i (2).

(2) medfører (3): Ses ved multiplikation til venstre med S på begge sider i ligningen i (2).

(3) medfører (4): Ses ved at konstatere at matricerne i (3) opfylder betingelserne i (4): Vi sætter $\lambda_i = D_{ii}$. På den ene side får vi da at $(SD)^j = SD^j = S\lambda_j E^j = \lambda_j SE^j = \lambda_j S^j$, og på den anden at $(AS)^j = AS^j$, tilsammen altså at $AS^j = \lambda_i S^j$.

(4) medfører (1): Vi har allerede vist at søjlerne i S er egenvektorer og antagelsen om at S er invertibel sikrer at de udgør en basis. Dette kriterium giver os altså også en opskrift på S og D.

Når vi skal diskutere muligheden for diagonalisering benyttes som som regel det første af kriterierne. Det er derfor nyttigt at vide følgende:

12. Sætning: Egenrummene er uafhængige

Hvis du tager en basis for hvert egenrum og slår dem sammen så får du en lineært uafhængig mængde.

Bevis : Lad Λ være en mængde af egenværdier. For hvert $\lambda \in \Lambda$ antager vi at B_λ er en basis for $E(\lambda)$ og sætter $B = \bigcup_{\lambda\in\Lambda} B_\lambda$. Vi vil vise at B er lineært uafhængig.

Vi fører beviset ved induktion efter størrelsen af Λ. Hvis der kun er 1 egenværdi i Λ er der intet at bevise. Vi antager nu at sætningen er bevist når Λ indeholder $r-1$ egenværdier og antager at Λ indeholder r egenværdier.

Antag således at $\sum_{v\in B} a_v v = 0$. *Vi skal da blot vise at* $a_v = 0$ *for alle* $v \in B$. *Lad* $\mu \in \Lambda$. *Vi har da at*

$$\begin{aligned} 0 =&(A-\mu E)\sum_{v\in B} a_v v = \sum_{v\in B} a_v (A-\mu E)v = \sum_{\lambda\in\Lambda}\sum_{v\in B_\lambda} a_v(A-\mu E)v \\ =&\sum_{\lambda\in\Lambda}\sum_{v\in B_\lambda} a_v(\lambda-\mu)v = \sum_{\lambda\in\Lambda,\lambda\neq\mu}\sum_{v\in B_\lambda} a_v(\lambda-\mu)v \end{aligned} .$$

Af induktionsantagelsen følger da at $a_v = 0$ *når* $v \notin B_\mu$. *Når dette indsættes i den første antagelse fås at* $\sum_{v\in B_\mu} a_v v = 0$ *og da* B_μ *er en basis fås da at* $a_v = 0$ *for* $v \in B_\mu$. *Dermed har vi vist at* $a_v = 0$ *for alle* $v \in B$ *og det viser at* B *er lineært uafhængig.*

Hvis vi benytter dette resultat for $\Lambda = \sigma(A)$ *fås resultatet i sætningen.* Denne sætning fører umiddelbart til

13. Sætning: Diagonaliserbarhed og geometrisk multiplicitet

En $n \times n$ *matrix* A *er diagonaliserbar hvis og kun hvis summen af dens geometriske multipliciteter er* n

14. Sætning: Den geometriske multiplicitet overstiger aldrig den algebraiske

Lad λ *være en egenværdi for* A. *Da er* $\mathrm{geo}(\lambda) \leq \mathrm{alg}(\lambda)$

15. Sætning: Diagonaliserbarhed kræver fuld algebraisk multiplicitet

En nødvendig betingelse for at en $n \times n$ *matrix* A *er diagonaliserbar er at summen af dens algebraiske multipliciteter er* n.

16. Sætning: Diagonaliserbarhed for de komplekse tal

Hvis $L = \mathbb{C}$, *så er en matrix diagonaliserbar hvis og kun hvis dens geometriske og den algebraiske multipliciteter er ens for enhver egenværdi*

4: Epilog

Du skulle efter læsningen vide at mange resultater fra teorien om reelle vektorrum har mening og gyldighed for vilkårlige legemer, men godt kan fremtræde væsentlig forskelligt fra mønstereksemplet.

Du skulle også vide at nogle resultater ikke kan overføres. Det gælder først og fremmest det som er knyttet til et indre produkt. Det gælder også de ting som er knyttet til at algebraens fundamentalsætning kun gælder i de komplekse tal, hvilket har betydning, når det drejer sig om diagonalisering af matricer.

Til perspektivering:

Vektorrum tjener selv som eksempel på en algebraisk struktur, hvis man udvider dette begreb til at omfatte mere end en slags objekter og operationer på mere end en slags objekter. De to slags objekter er vektorer og skalarer og den ekstra operation er multiplikation af vektor med skalar.

5: Eksempler og øvelser

Eksempel 1: Dellegemer
En delmængde af et legemer som er lukket mht de fire regneoperationer er et legeme. Dette kan nemt vises (Ø2).

Delmængden $\mathbb{Q} + \sqrt{2}\mathbb{Q} = \{p + q\sqrt{2} : p, q \in \mathbb{Q}\}$ af de reelle tal er et dellegeme. At se at denne mængde er lukket overfor division kan gøres ved at bruge det gamle trick til bortskaffelse af nævnere med rødder:

$$\frac{a + \sqrt{2}b}{c + \sqrt{2}d} = \frac{(a + \sqrt{2}b)(c - \sqrt{2}d)}{(c + \sqrt{2}d)(c - \sqrt{2}d)} = \frac{ac - 2bd + (-ad + bc)\sqrt{2}}{c^2 - 2d^2}$$

Øvelse 2: Dellegemer
Vis den indledende påstand i E1

Øvelse 3: xrsDellegemer2
Hvad er det mindste legeme som indeholder både $\sqrt{2}$ og $\sqrt{3}$?

Eksempel 4: Ligninger med komplekse ubekendte
På næste side er anført stadierne i en gausselmination som viser hvordan man kan løse ligningssystemet

$$\begin{aligned} 2x + 3y + iz &= i \\ ix + y + 3z &= 2 \\ (2 + i)x + 4y + (3 + i)z &= 2 + i \end{aligned}$$

.

Der er givet koefficientmatricen $A =$

$$\begin{pmatrix} 2 & 3 & i \\ i & 1 & 3 \\ 2+i & 4 & 3+i \end{pmatrix}$$

som ved tilføjelse af enhedsmatrix giver $A_0 =$

$$\begin{pmatrix} 2 & 3 & i & 1 & 0 & 0 \\ i & 1 & 3 & 0 & 1 & 0 \\ 2+i & 4 & 3+i & 0 & 0 & 1 \end{pmatrix}$$

Ved addition til række nr 2 af $-\frac{i}{2}$ gange række nr 1 fås

$$\begin{pmatrix} 2 & 3 & i & 1 & 0 & 0 \\ 0 & 1-\frac{3i}{2} & \frac{7}{2} & -\frac{i}{2} & 1 & 0 \\ 2+i & 4 & 3+i & 0 & 0 & 1 \end{pmatrix}$$

Ved addition til række nr 3 af $-1-\frac{i}{2}$ gange række nr 1 fås

$$\begin{pmatrix} 2 & 3 & i & 1 & 0 & 0 \\ 0 & 1-\frac{3i}{2} & \frac{7}{2} & -\frac{i}{2} & 1 & 0 \\ 0 & 1-\frac{3i}{2} & \frac{7}{2} & -1-\frac{i}{2} & 0 & 1 \end{pmatrix}$$

Ved addition til række nr 3 af -1 gange række nr 2 fås

$$\begin{pmatrix} 2 & 3 & i & 1 & 0 & 0 \\ 0 & 1-\frac{3i}{2} & \frac{7}{2} & -\frac{i}{2} & 1 & 0 \\ 0 & 0 & 0 & -1 & -1 & 1 \end{pmatrix}$$

Ved multiplikation af række nr 2 med $\frac{4}{13}+\frac{6i}{13}$ fås

$$\begin{pmatrix} 2 & 3 & i & 1 & 0 & 0 \\ 0 & 1 & \frac{14}{13}+\frac{21i}{13} & \frac{3}{13}-\frac{2i}{13} & \frac{4}{13}+\frac{6i}{13} & 0 \\ 0 & 0 & 0 & -1 & -1 & 1 \end{pmatrix}$$

Ved addition til række nr 1 af -3 gange række nr 2 fås

$$\begin{pmatrix} 2 & 0 & -\frac{42}{13}-\frac{50i}{13} & \frac{4}{13}+\frac{6i}{13} & -\frac{12}{13}-\frac{18i}{13} & 0 \\ 0 & 1 & \frac{14}{13}+\frac{21i}{13} & \frac{3}{13}-\frac{2i}{13} & \frac{4}{13}+\frac{6i}{13} & 0 \\ 0 & 0 & 0 & -1 & -1 & 1 \end{pmatrix}$$

Ved multiplikation af række nr 1 med $\frac{1}{2}$ fås

$$\begin{pmatrix} 1 & 0 & -\frac{21}{13}-\frac{25i}{13} & \frac{2}{13}+\frac{3i}{13} & -\frac{6}{13}-\frac{9i}{13} & 0 \\ 0 & 1 & \frac{14}{13}+\frac{21i}{13} & \frac{3}{13}-\frac{2i}{13} & \frac{4}{13}+\frac{6i}{13} & 0 \\ 0 & 0 & 0 & -1 & -1 & 1 \end{pmatrix}$$

Matricen for løselighedsbetingelsen er

$O_2 = (-1 \quad -1 \quad 1)$

Ved at udtage de første 2 rækker fås

$$\begin{pmatrix} 1 & 0 & -\frac{21}{13}-\frac{25i}{13} & \frac{2}{13}+\frac{3i}{13} & -\frac{6}{13}-\frac{9i}{13} & 0 \\ 0 & 1 & \frac{14}{13}+\frac{21i}{13} & \frac{3}{13}-\frac{2i}{13} & \frac{4}{13}+\frac{6i}{13} & 0 \end{pmatrix}$$

$\{1, -i, 1-i\}$

Betingelsen for løselighed kan checkes ved at se på

$$(-1 \quad -1 \quad 1)\begin{pmatrix} 1 \\ -i \\ 1-i \end{pmatrix} = (0)$$

Basis variable er $\{1, 2\}$

Frie variable er $\{3\}$

Ved permutering af søjler fås reduceret normalform

$$\begin{pmatrix} 1 & 0 & -\frac{21}{13}-\frac{25i}{13} & \frac{2}{13}+\frac{3i}{13} & -\frac{6}{13}-\frac{9i}{13} & 0 \\ 0 & 1 & \frac{14}{13}+\frac{21i}{13} & \frac{3}{13}-\frac{2i}{13} & \frac{4}{13}+\frac{6i}{13} & 0 \end{pmatrix}$$

En (omordnet) basis for nulrummet er søjlerne i matric

$$\begin{pmatrix} \frac{21}{13}+\frac{25i}{13} \\ -\frac{14}{13}-\frac{21i}{13} \\ 1 \end{pmatrix}$$

Matricen til modificering af højresiden er

$$O_1 = \begin{pmatrix} \frac{2}{13}+\frac{3i}{13} & -\frac{6}{13}-\frac{9i}{13} & 0 \\ \frac{3}{13}-\frac{2i}{13} & \frac{4}{13}+\frac{6i}{13} & 0 \end{pmatrix}$$

En (omordnet) partikulær løsning er

$$\begin{pmatrix} -\frac{7}{13}+\frac{9i}{13} \\ \frac{9}{13}-\frac{6i}{13} \\ 0 \end{pmatrix}$$

En (omordnet) basis for nulrummet er søjlerne i matric

$$\begin{pmatrix} \frac{21}{13}+\frac{25i}{13} \\ -\frac{14}{13}-\frac{21i}{13} \\ 1 \end{pmatrix}$$

Øvelse 5: Inversion af kompleks matrix
Lad A være matricen

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}.$$

Bestem A^{-1} direkte f.eks. vha Gauss-Jordan metoden. Vis at $A^{-1} = \bar{A}$.

Øvelse 6: Inversion af kompleks matrix
Lad n være et naturligt tal og sæt $z = e^{\frac{2\pi i}{n}}$, en af løsningerne til ligningen $z^n = 1$. Lad F_n være den matrix som i række nr r og søjle nr s har elementet $a_{rs} = \frac{1}{\sqrt{n}} z^{rs}$, hvor rækker og søjler nummereres fra 0 til $n-1$.

Vis at $A = F_n$, for $n = 4$, hvor A er matricen i Ø5

Vis at $F_n^{-1} = \bar{F_n}$ for alle n

Opskriv F_3 og F_3^{-1}.

Øvelse 7: Fourier-matrix
Matricen F_n i Ø 6 kaldes for Fourier-matricen af orden n og den tilhørende lineære afbildning kaldes for den diskrete Fouriertransformation.

Hvis $x, y \in \mathbb{C}^n$ og $y = F_n x$ da er

$$y_r = \sum_{s=0}^{n-1} x_s e^{\frac{2\pi rsi}{n}},$$

og vi at y er den Fouriertransformerede af x. Vis Fouriers inversionsformel, der genfinder x ud fra sin Fouriertransformerede:

$$x_r = \sum_{s=0}^{n-1} y_s e^{\frac{-2\pi rsi}{n}}.$$

Eksempel 8: Inversion af matrix i $\mathbb{Z}_3$

Vi regner nu i legemet $\mathbb{Z}_3$, hvor følgende række af matrixomformninger

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 & 1 & 0 \\ 1 & 1 & -1 & 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 1 \end{pmatrix} \to$$
$$\begin{pmatrix} 1 & 1 & 0 & -1 & 0 & -1 \\ 0 & 1 & 0 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 & -1 & -1 \\ 0 & 1 & 0 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 1 \end{pmatrix} \to$$

viser at

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & -1 & -1 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}.$$

Undervejs har vi gjort flittigt brug af at $-2 = 1$ og $-1 = 2$.

Eksempel 9: Der findes flere endelige legemer
Lad L være en mængde bestående af fire elementer $0, 1, i, j$ og lad operationerne være givet ved tabellerne

+	0	1	i	j
0	0	1	i	j
1	1	0	j	i
i	i	j	0	1
j	j	i	1	0

·	0	1	i	j
0	0	0	0	0
1	0	1	i	j
i	0	i	j	1
j	0	j	1	i

Vis at i op j er løsninger til ligningen $x^2 + x + 1 = 0$.

Øvelse 10: Legeme som vektorrum over sig selv
Ethvert legeme er et vektorrum over sig selv. Fortolk denne påstand og eftervis den.

Eksempel 11: Legeme som vektorrum over dellegeme

1) De komplekse tal $\mathbb{C}$ er med oplagte definitioner af vektorrumsoperationer et vektorrum over de relle tal $\mathbb{R}$. Parret $(1, i)$ giver anledning til en basis. Koordinatsættet for det komplekse tal $x + iy$ mht denne basis er (x, y).
2) De reelle tal $\mathbb{R}$ udgør med oplagte definitioner et vektorrum over de rationale tals legeme $\mathbb{Q}$. Det kan vises, men det er overordentlig kompliceret (og involverer udvalgsaksiomet) at dette vektorrum har en basis og at det er uendeligdimensionalt.

Øvelse 12: Vektorrum af polynomier
En polynomiumsfunktion kan nemt defineres for vilkårlige legemer og mængden af polynomiumsfunktioner udgør et vektorrum.

Bestem samtlige polynomier når legemet er $\mathbb{Z}_2$ og vis på denne måde at enhver funktion af $\mathbb{Z}_2$ ind i sig selv er et polynomium.

Find en basis for dette vektorrum. Vis at det er isomorft med $\mathbb{Z}_2^2$. Hvad vil du sige om begrebet grad af polynomium i dette tilfælde?

Eksempel 13: A og $A^\perp$ er ikke komplementære
Lad $V = \mathbb{Z}_2^3$ udstyret med standardproduktet. Lad S være underrummet med ligningen $x = y$. Bestem $S^\perp$. Vi ser at S er nulrum for matricen $\begin{pmatrix} 1 & -1 & 0 \end{pmatrix}$ og vi finder nemt en basis. Anvendes basisvektorerne som søjler fås matricen

$$U = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Derfor vil $S^\perp$ være nulrum for matricen U^t. En basis for $S^\perp$ kan derfor findes: $(1, 1, 0)$. Vi ser således at $S^\perp$ er en delmængde af S.

Eksempel 14: Det pseudoortogonale underrum
Lad $V = \mathbb{Z}_3^2$ udstyret med standardproduktet. Lad S være underrummet med ligningen $x = y$. Bestem $S^\perp$. Vi ser at S er nulrum for matricen $\begin{pmatrix} 1 & -1 \end{pmatrix}$ og vi finder nemt en basis, bestående af den ene vektor $(1, 1)$. Lad U være matricen med denne ene søjle. Da vil $S^\perp$ være nulrum for matricen U^t. En basis for $S^\perp$ kan derfor findes: $(1, 2)$.

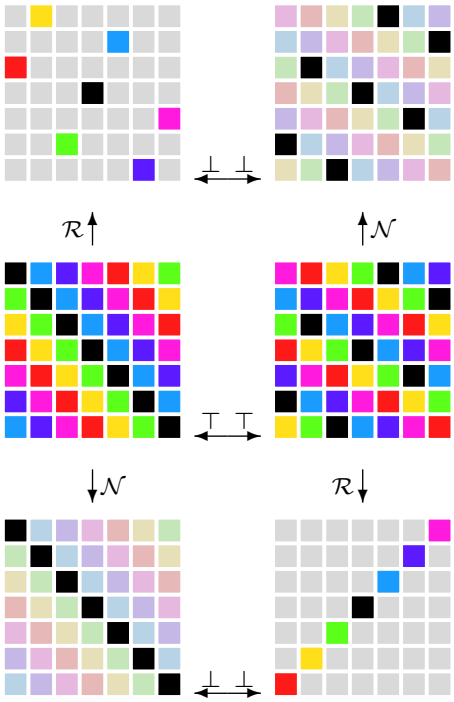
Eksempel 15: De fundamentale underrum
Vi arbejder i $\mathbb{Z}_7$. Der er givet matricen

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}.$$

Det er nemt at finde de fire fundamentale underrum. Disse er illustreret grafisk på figuren. Alle 6 diagrammer er $\mathbb{Z}_7^2$ med tallene $\{-3, -2, -1, 0, 1, 2, 3\}$ på begge akser. Hvert punkt er markeret med et farvelagt kvadrat. Diagrammerne i venstre kolonne refererer til A og dem i højre kolonne til $A^\top$. I rækken i midten illustrerer farverne afbildningens værdi i det enkelte punkt, værdien $(0, 0)$ svarer til farven sort. Der forekommer kun 7 forskellige billeder, da billedrummet har dimensionen 1.

Nulrummene er fremhævet i de diagrammer hvortil der fører en pil med $\mathcal{N}$. Billedrummene svarer på tilsvarende måde til pile med $\mathcal{R}$. I disse er det de enkelte punkter i billedrummet som er markeret med den farve der kendetegner punktet.

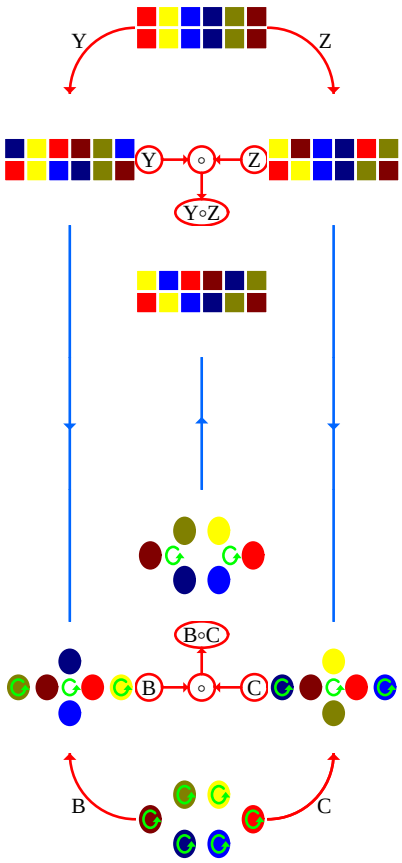
De vandrette pile markerer at de to underrum på begge sider er pseudoortogonale. Der er en vis geometrisk understøttelse for dette formelle faktum.



Øvelse 16: Man tager en matrix
Vælg en 3×5- matrix A hvis elementer er hele tal $z \in \mathbb{Z}$ som opfylder $|z| \leq 2$. Opfat dette som en matrix over $\mathbb{Z}_2$ og bestem de fire fundamentale underrum $\mathcal{N}(A)$, $\mathcal{R}(A)$, $\mathcal{N}(A^\top)$, $\mathcal{R}(A^\top)$. Gør det samme over andre endelige legemer.

Anders Madsen

PERMUATIONER



ABSTRAKTE ALGEBRAISKE STRUKTURER

6

Dette er et hæfte i en serie med titlen "Konkrete algebraiske strukturer", som jeg har skrevet til algebrakurset (E1) på matematikuddannelsen ved IMFUFA på RUC.

Hæfterne skal ses i sammenhæng med en anden serie hæfter med titlen "Abstrakte algebraiske strukturer". Disse to serier udgør hver sin kæbe i en knibtang.

Naturligvis ville det være tomt (og frustrerende) at undervise i abstrakt algebra uden inddragelse af konkrete eksempler og det ville være fattigt (og perspektivforladt) kun at gennemgå konkrete eksempler uden at inddrage de underliggende abstrakte strukturer.

På den anden side er der en vis skønhed i at fremhæve den abstrakte karakter ved at isolere den og lade dens top-down karakter fremstå tydeligt som i det forkætrede forbillede "Matematikens elementer" af Bourbaki. Starte med de groveste strukturer og efterhånden tilføje finere strukturelementer. Alle resultater, som går igen og igen, formuleres og bevises en gang for alle.

Ligeledes er der en tilfredsstillelse forbundet med at lade de enkelte konkrete strukturer stå så enkelt som muligt, uden overflødige dikkedarer, das Ding an sich. Og der er fornøjelsen ved at se det essentielt samme argument komme igen og igen i forskellige forklædninger.

Udover den æstetiske tilfredstillelse ved den rene abstraktion og den rene fornøjelse ved de konkrete detaljer har begge disse perspektiver en stor erkendelsesmæssig betydning og bidrager til udviklingen af kompetencer som er væsentlige for matematikere.

Jeg har valgt at fremhæve de to modsatrettede men samspillende perspektiver ved den opdeling som de to serier repræsenterer. De enkelte konkrete strukturer er fremstillet i enkeltstående fremstillinger uden indbyrdes referencer. Stof som forudsættes flere steder er medtaget hvert sted. Men udvalget af detaljer er foretaget på en sådan måde at det bedst muligt kan levere stof til den abstrakte del.

Den matematiske kerne for de enkelte hæfter, uden forbindende tekst og illustrationer, har foreligget tidligere i mere rå form beregnet på uddybning ved forelæsning og ikke egnet til selvstudium, ikke mindst på grund af utallige trykfejl og tanketorsk, som de studerende med stor tålmodighed har fanget. Dette skylder jeg dem tak for og derfor er hæfterne tilegnet alle tidligere og nuværende studerende på E1, som jeg takker for deres medvirken.

Hefterne findes i netudgaver med alle referencer som aktive links og med opdateringer:

Anders Madsen, december 2006

Indholdsfortegnelse

1: Prolog

I dette hæfte skal du (gen)se et konkret eksempel på en algebraisk struktur. Vi taler om en algebraisk struktur, når vi har en bestemt type objekter og en eller flere operationer på denne type objekter, der fører til et objekt af samme type, samt nogle regneregler for disse operationer.

Det mest oplagte eksempel har som objekter de reelle tal, som operationer de sædvanlige aritmetiske operationer med de sædvanlige regneregler.

Her skal vi se nærmere på den algebraiske struktur, der har permutationer som sine objekter og sammensætning og invertering af bijektive afbildninger som operationer. Vi skal gennemføre de overvejelser, som fører til at man kan inddele permutationer i lige og ulige permutationer, altså tildele dem en paritet, og finde metoder til at bestemme pariteten.

Hovedredskaberne er forskellige faktoriseringer af permutationer. Faktorisering optræder i mange konkrete algebraiske strukturer, hvor vilkårlige objekter forsøges udtrykt ved operationen anvendt på specielt simple objekter. Mønstereksemplert er faktoriseringen af et vilkårligt naturligt tal som produkt af primtal. Der vil være en opsamling med tydeligørelse af den røde tråd i epilogen.

2: Baggrund og definitioner

2.1: Permutationer som modeller

Permutation betyder ombytning. På engelsk optræder ordet i denne betydning i dagligsproget. På dansk er det et fremmedord. Det bruges i matematikken om de matematiske objekter som kan anvendes til at modellere en ombytning af rækkefølgen af et vist endeligt antal objekter.

Lad der være givet et endeligt antal elementer, som er anbragt på et endeligt antal pladser. Vi kan lave en oplagt matematisk model af dette ved at tage en en mængde X hvis elementer modellerer pladserne, en mængde A, hvis elementer modellerer objekterne og en bijektiv afbildning $\alpha : A \to X$ som modellerer placeringen af objekterne, således at $\alpha(a)$ betegner den plads hvorpå objektet a er anbragt.

En anden placering af de samme objekter på de samme pladser vil da være modelleret ved en anden bijektiv afbildning $\beta : A \to X$.

Hvis vi tænker os at placeringen givet vha β er fremkommet ved en omordning af placeringen givet vha α, da kan vi angive denne omordning ved til en given placering $x \in X$ at knytte den plads som efter omordningen er plads for det objekt der inden omordingen har pladsen x. Vi ser at denne afbildning af X ind i sig selv er givet som $\beta \circ \alpha^{-1}$.

Vi kan også angive omordningen ved til et givet objekt a at knytte det objekt som efter omordningen befinder sig på den plads som a befandt sig på før omordningen. Vi ser at denne afbildning af A ind i sig selv er givet som $\beta^{-1} \circ \alpha$.

Vi ser at omordningen i begge situationer kan modelleres vha en enkelt bijektiv afbildning af en endelig mængde ind i sig selv.

Alt i alt er dette baggrunden for følgende definition.

2.2: Permutation som matematisk objekt

1. Definition: Permutation

Lad A være en endelig mængde, som ikke er tom. En bijektiv afbildning af A på sig selv kaldes en permutation [af A].

Hvis $(a_1, \ldots, a_n)$ er en indicering af elementerne i A, da vil en permutation p kunne angives entydigt ved symbolet

$$\begin{pmatrix} a_1 & \ldots & a_n \\ b_1 & \ldots & b_n \end{pmatrix},$$

hvor $b_i = p(a_i), i = 1, \ldots, n$.

Der er simple eksempler på permutationer i E1 Ø2 Ø3 Ø4 Ø5 Ø6 Ø7

2.3: Operationer på permutationer

Hvis vi har to permutationer f og g da er sammensætningen $g \circ f$ også en permutation og det er nemt at se at den er udtryk for den omordning som fremkommer ved først at anvende omordningen svarende til g og dernæst at anvende omordningen svarende til g på resultatet. Vi har derfor følgende

2. Definition: Produkt, invers, identiteten

Lad f og g være permutationer af A. Vi kalder da sammensætningen $g \circ f$ for permutationsproduktet af g og f, som vi også (af gammel tradition og af

bekvemmelighed) skriver gf. Ofte vil vi nøjes med at sige produkt i stedet for permutationsprodukt. Den identiske afbildning af A kaldes den identiske permutation, eller identiteten og den inverse afbildning af en permutation kaldes den inverse permutation eller blot den inverse. Vi benytter også sædvanlig potensskrivemåde f^n for alle $n \in \mathbb{Z}$ i overensstemmelse med sædvanlig skrivemåde for potenser af (bijektive) afbildninger.

Permutationsproduktet er interessant for analysen af permutationer fordi vilkårlige permutationer kan skrives som produkt af særligt simple permutationer, kaldet cykliske permutationer. Det følgende handler først og fremmest om denne "faktorisering", som har visse paralleller til faktorisering af hele tal som produkt primtal.

3: Cykliske permutationer

3.1: Permutation som dynamik

Vi vil til det formål benytte os af endnu en fortolkning af hvad en permutation er, idet vi tænker på de givne genstande, elementerne i A, som de mulige tilstande et vist system kan befinde sig i. En afbildning p af tilstandsmængden ind i sig selv kan da opfattes som en beskrivelse af en dynamik, hvor relationen $y = p(x)$ udtrykker at hvis systemet til et vist tidspunkt befinder sig i tilstanden x da vil det til det næste tidspunkt befinde sig i tilstanden y. Dette forudsætter at det har mening at tale om det næste tidspunkt, hvilket for eksempel er tilfældet hvis de mulige tidspunkter kan angives ved hjælp af de naturlige tal. For denne fortolkning er det ikke vigtigt at p er en bijektion. Hvis vi derimod også forlanger at systemet kun kan være kommet i en bestemt tilstand på et vist tidspunkt, hvis det har været i en bestemt anden tilstand til det forudgående tidspunkt, da må p være en bijektion altså en permutation. De næste definitioner knytter an til denne fortolkning af en permutation.

---

3. Definition: Bane

Lad p være en permutation af A og a et element i A. Mængden $\{a, p(a), p^2(a), \ldots\}$ kaldes banen for a mht til p og skrives $\langle a \rangle_p$.

Ø8

---

4. Definition: Cykel

Et ordnet sæt $(a_1, \ldots, a_k)$ af elementer i A kaldes en cykel af længde k eller blot en k-cykel for permutationen p, hvis det gælder at $p(a_i) = a_{i+1}$ for alle $p = 1, \ldots, k-1$ og $p(a_k) = a_1$, og det samtidigt gælder at k er det mindste positive hele tal for hvilket dette gælder. Vi udvider definitionen til også at omfatte $k = 0$, idet $(a_1, \ldots, a_k)$ i dette tilfælde skal stå for det tomme ordnede sæt $(\,)$.

---

5. Sætning: Banen for en cykel

Lad $(a_1, \ldots, a_k)$ være en k-cykel. Da vil alle a_i have samme bane, nemlig $\{a_1, \ldots, a_k\}$. Dette omfatter også $k = 0$ hvor banen er den tomme mængde

---

6. Definition: Banen for en cykel

Den i sætningen nævnte fælles bane kaldes banen for den pågældende cykel.

---

7. Definition: Fixpunkt

Hvis $p(a) = a$ så kaldes a for et fixpunkt for p, (engelsk fixed point)

Exersize Oktaeder, drejning 90 om axe gennem modstillede hjørner. Find Fixpunkter og Støtte og samtlige baner

---

8. Definition: Berørt og uberørt del, støtte og fixpunktmængde

Lad p være en permutation af A. Vi sætter da

$$\mathrm{Fix}(p) = \{a \in A : p(a) = a\}$$
$$\mathrm{St}(p) = \{a \in A : p(a) \neq a\}$$

Vi kalder $\mathrm{Fix}(p)$ for fixpunktmængden for p og $\mathrm{St}(p)$ for støtten for p. Vi vil (i nærværende sammenhæng) også tale om den af p uberørte, henholdsvis berørte del.

3.2: cykliske permutationer

---

9. Definition: Cyklisk permutation

En permutation kaldes cyklisk, hvis den berørte del udgøres af en banen for en cykel. Hvis den berørte del er banen for cyklen $(a_1, \ldots, a_k)$ vil vi notere p med $(a_1 \cdots a_k)$.

10. Bemærkning : Samme cykliske permutation svarer til flere cykler

Bemærk at en cyklisk permutation af længde større end 1 *svarer til flere cykler. Bemærk også at betegnelsen* $(a_1 \dots a_k)$ *står for den cykliske permutation. Vi har altså at de to cykliske permutationer* (123) *og* (231) *er identiske mens cyklerne* $(1, 2, 3)$ *og* $(2, 3, 1)$ *er forskellige. Vi skelner altså mellem cykler og cykliske permutationer. Det vil dog ikke føre til slemme misforståelser hvis man glemmer at skelne.*

11. Definition: Disjunkte permutationer

To permutationer kaldes disjunkte hvis deres berørte dele,altså deres støtter, er disjunkte

12. Definition: Invariant mængde

Lad A' *være en delmængde af* A *og* p *en permutation af* A*. Hvis* $p(A') = A'$ *da siger vi at* A' *er invariant mht* p*.*

13. Sætning: Restriktion og udvidelse

Antag at $A' \subseteq A$ *og* p *er en permutation af* A*. Hvis* A' *er invariant mht til* p*, da er restriktionen* p' *af* p *til* A' *en permutation af* A'*. Hvis* p' *er en permutation af* A' *og* p *er den afbildning af* A *ind i sig selv som stemmer overens med* p' *i* A' *og stemmer overens med identiteten uden for* A' *da er* p *en permutation af* A

Bevis : Vi har per definition at p' *er en afbildning af* A' *ind i sig selv. Da* p *er injektiv må også* p' *være injektiv. Derfor har* $p'(A')$ *det samme antal elementer som* A'*. Og da* $p'(A') \subseteq A'$ *så må* $p'(A') = A'$*, så* p' *altså også er surjektiv. (Vi har vist at en injektiv afbildning af en endelig mængde ind i sig selv er automatisk surjektiv). Alt i alt er* p' *bijektiv.*

14. Definition: Restriktion og udvidelse

Når situationen er som i sætningen siger vi at p' *er restriktionen eller indskrænkningen af* p *til* p'*. Når* p *er dannet ud fra* p' *som beskrevet så siger vi at* p *er den kanoniske udvidelse af* p' *til* A

3.3: Faktorisering i disjunkte cykler

15. Sætning: Struktursætning

Enhver permutation kan skrives som produkt af disjunkte cykliske permutationer

Bevis : *Vi kan angive følgende (rekursive) algoritme til angivelse af en liste af disjunkte cykliske permutationer som postuleret i sætningen. En rekursiv er en som må bruge sig selv på en sådan måde at det alligevel ikke kører i ring fordi den bruges i situationer hvor den "allerede" er defineret.*

Hvis p allerede er cyklisk er vi naturligvis færdige.

Hvis p ikke er cyklisk gøres følgende

1) *Vælg $a_1 \in A$*

2) *Lad p_1 være den cykliske permutation, der som sin bane har banen for a_1.*

3) *Lad A' være mængden af elementer som ikke ligger i banen for for a_1 og lad p' være den permutation af A' som er restriktionen af p til A'.*

4) *Benyt algoritmen (som vi er ved at definere!) til at skrive p' som produkt $p'_2 \cdots p'_r$ af cykliske permutationer i A'.*

5) *Lad for hvert $i = 2, \ldots, k$ p_i være den kanoniske udvidelse af p'_i fra A' til A.*

6) *Resultatet af algoritmen er da at $p = p_1 \cdots p_n$ er en fremstilling af p som produkt af disjunkte permutationer.*

For at bevise at denne algoritme i alle tilfælde giver det ønskede resultat benytter vi induktion mht antallet, n, af elementer i A.

Hvis $n = 1$ er p nødvendigvis selv en en cyklisk permutation, og sagen derfor klar.

Antag nu at sætningen for et vist $k > 1$ allerede er bevist for alle n der opfylder $n < k$; vi vil vise at sætningen også gælder for $n = k$, og antager altså at A har k elementer. Hvis vi er i den første forgrening i algoritmen er vi færdige. Lad os derfor antage at vi er i den anden forgrening af algoritmen, altså at p ikke selv er cyklisk.

Vi kan udføre punkt 1 fordi A per definition ikke er tom.

Vi kan udføre punkt 2 fordi cyklen på oplagt vis giver anledning til en permutation af sin bane og p_1 er den kanoniske udvidelse af denne permutation til A.

Vi kan udføre punkt 3 fordi A' ikke er tom, hvilket følger af at p ikke er cyklisk.

At også punkt 4 kan udføres følger af induktionsantagelsen eftersom antallet af elementer i A' må være mindre end k.

Punkt 5 er uden problemer.

Vi mangler nu blot at vise at $p = p_1 \cdots p_r$. Dette virker heldigvis oplagt, men lad os alligevel gå noget i detaljer.

Vi ser først på et vilkårligt a i den af a_1 frembragte cykel. Da er det klart af definitionen at $p_i(a) = a$ for alle $i > 1$ da a ikke ligger i A'. Derfor er også $(p_2 \cdots p_r)(a) = a$ og følgelig er $(p_1 \cdots p_k)(a) = p_1(p_2 \cdots p_k(a)) = p_1(a) = p(a)$.

Vi ser dernæst på et vilkårligt a i A'. Vi har da at $p_2 \cdots p_r(a) = p'_2 \cdots p'_r(a) = p'(a) = p(a)$ og følgelig at $(p_1 \cdots p_r)(a) = p_1(p(a)) = p(a)$, det sidste lighedstegn fordi $p(a)$ tilhører A' og derfor er et fixpunkt for p_1.

Da vi dermed for alle a har vist at $(p_1 \cdots p_r)(a) = p(a)$ er beviset fuldført.

16. Bemærkning : En iterativ algoritme

Den her anførte algoritme er rekursivt formuleret, fordi det er elegant og praktisk især mht beviset. Det er dog klart at følgende iterativt formulerede algoritme dækker det samme og er nemmere at anvende:

Vælg et element, bestem dets cykel og anse dennes elementer for at være taget. Vælg dernæst et element som ikke allerede er taget, bestem så dettes cykel og anse og dennes elementer for at være taget. Fortsæt på denne måde indtil alle elementer er taget. De ønskede faktorer er da de cykliske permutationer, som er bestemt af de successivt udvalgte cykler.

17. Eksempel: Find faktoriseringen i disjunkte cykler

Lad

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 5 & 4 & 1 \end{pmatrix}.$$

Vi illustrerer først den rekursive metode. Vi starter med at vælge $a_0 = 1$*, som giver cyklen*$(1, 3, 6)$*.*

Vi har da restmængden $A' = \{2, 4, 5\}$ *hvorpå vi har permutationen*

$$p' = \begin{pmatrix} 2 & 4 & 5 \\ 2 & 5 & 4 \end{pmatrix}.$$

Vi skal nu bruge vores algoritme på p'*. Vi sætter derfor* $A = A'$ *og* $p = p'$ *og vælger* $a_0 = 2$ *der giver anledning til cyklen* (2) *.*

Som ny restmængde fås $A' = \{4, 5\}$ *med*

$$p' = \begin{pmatrix} 4 & 5 \\ 5 & 4 \end{pmatrix}.$$

Vi sætter igen $A = A'$ *og* $p = p'$ *og vælger* $a_0 = 4$ *som nyt udgangspunkt, hvilket giver anledning til cyklen* $(4, 5)$*. Vi har da at* $p = (136)(2)(45)$*.*

Den iterative algoritme illustreres på følgende måde:

Vælg elementet 1 og tag elementerne i den tilhørende cykel $(1, 3, 6)$. Vi har så ikke endnu taget $2, 4, 5$. Vi vælger 2 og tager elementerne i den tilsvarende cykel, som er (2). Nu mangler vi $4, 5$. Vi vælger 4, den tilsvarende cykel er $(4, 5)$. Nu mangler der ikke mere, så fremstillingen er $(136)(2)(45)$.

18. Bemærkning : Regning med cykler.

Antag at du skal beregne et produkt af permutationer, idet du allerede har spaltet de enkelte faktorer som produkt af disjunkte cykler. Da er det nemt at udregne produktet. Vi kan jo finde virkningen af $pq = p_1 \cdots p_r q_1 \cdots q_s \cdots$ *på* $a \in A$ *ved at opsøge den bagerste cykel som a forekommer i, notere resultatet b af dennes virkning på a og derefter gå til den nærmest foranstående permutation hvori b forekommer og se hvad denne gør ved b. Og siden fortsætte på denne måde indtil vi er kommet hele vejen igennem.*

Metoden kan ses i detaljer i Ø9

---

19. Definition: Cyklisk notation

Vi siger at en permutation er skrevet i cyklisk notation hvis den er skrevet som produkt af disjunkte cykliske permutationer.

Ø10 Ø11

Vi kommer nu til en vigtig anvendelse af faktorisering af permutationer i faktorer som er cykliske permutationer, nemlig inddelingen af permutationerne i lige og ulige permutationer, en inddeling som har stor betydning ved udregningen af determinanter og ved regning med orienteringer.

3.4: Faktorisering i 2-cykler

20. Sætning: Faktorisering i 2-cykler

Enhver permutation er produkt af 2-cykliske permutationer

Bevis : *Da enhver permutation er et produkt af cykliske permutationer er det nok at vise at enhver cyklisk permutation er produkt af 2-cykliske permutationer. Dette ses direkte af formlen*

$$(a_1 \cdots a_k) = (a_1\, a_2)(a_2\, a_3)\cdots(a_{k-1}\, a_k),$$

som eftervises ved inspektion af virkningen på hvert enkelt element.

Ethvert helt tal er jo lige eller ulige. Denne egenskab ved tallet kaldes dets paritet.

21. Sætning: Pariteten af antal 2-cykler

Antallet af faktorer i alle produkter af 2-cykler som som har et givet produkt har samme paritet

Bevis : *Lad os starte med at vise at den identiske permutation, $(\,)$, ikke kan skrives som et produkt af et ulige antal 2-cykler. Vi gør dette ved at vise at antallet af faktorer i et sådant produkt altid kan reduceres med to, hvis det da ikke kun består af en enkelt faktor. Så lad $p_1, \ldots p_k$ være 2-cykler således at $(\,) = p_1 \cdots p_k$, hvor $k > 1$. Lad x og y være de to elementer som bestemmer p_1, altså $p_1 = (x\, y)$. Vi vil se på hvordan vi kan flytte en 2-cykel som indeholder x fremad i rækkefølgen af faktorer. Lad derfor p_i være en 2-cykel af formen $(x\, z)$ og antag at p_{i-1} har formen $(u\, v)$ hvor både u og v er forskellige fra x. Vi har da at*

$$p_{i-1}p_i = (u\, v)(x\, z) = \begin{cases} (x\, v)(u\, v) & \text{for } z = u \\ (x\, u)(u\, v) & \text{for } z = v \\ (x\, z)(u\, v) & \text{for } z \neq u, z \neq v \end{cases}$$

(dette kan i alle tre tilfælde nemt checkes ved udregning af begge sider af ligningen.) Derfor kan man altså erstatte et par $p_{i-1}p_i$ hvor den forreste ikke indeholder x mens den bagerste gør med et andet par $q_{i-1}q_i$, hvor det nu kun er den forreste som indeholder x, uden at det samlede produkt ændres. Ved at anvende denne procedure gentagne gange kan vi altså nå frem til at skrive

$$(\,) = (x\,y)r_2 \cdots r_l s_{l+1} \cdots s_k,$$

hvor alle r_i indeholder x mens ingen s_i indeholder x. Hvis $l = k$ bortfalder s'erne. Bemærk at $l > 1$. Vi har altså at det for passende $a_2, \ldots, a_l$ gælder at

$$(\,) = (x\,y)(x\,a_2)\ldots(x\,a_l)s_{l+1} \cdots s_k$$

Nu kan vi se at mindst et af elementerne a_i må være y ved at udnytte at $(\,)(x) = x$. (Hvis y ikke forekom blandt a'erne ville $(\,)(x) = y$. Lad os lade i være den mindste værdi for hvilken $a_i = y$ således at

$$(\,) = (x\,y)(x\,a_2)\ldots(x\,a_{i-1})(x\,y)(x\,a_{i+1})\ldots(x\,a_l)s_{l+1} \cdots s_k$$

Her kan højresiden endda ved en række omkostningsfri tilføjelser af $(x\,y)(x\,y)$ omskrives til

$$(x\,y)(x\,a_2)(x\,y)(x\,y)(x\,a_3)(x\,y)\ldots(x\,y)(x\,a_{i-1})(x\,y)(x\,a_{i+1})$$
$$\ldots(x\,a_l)s_{l+1} \cdots s_k$$

Da $(x\,y)(x\,a_j)(x\,y) = (y\,a_j)$ for $j = 2, \ldots, i-1$ har vi altså at

$$(\,) = (y\,a_2)\ldots(y\,a_{i-1})(x\,a_{i+1})\ldots(x\,a_l)s_{l+1} \cdots s_k$$

hvilket er en fremstilling af $(\,)$ som produkt af $k-2$ 2-cykliske permutationer.

Dermed er det postulerede resultat for den identiske permutation eftervist, nemlig at enhver fremstilling af den som produkt af 2-cykliske permutationer må have et lige antal faktorer.

Lad os som forberedelse til det generelle resultat bemærke at hvis en permutation er produkt af 2-cykliske faktorer, da er den inverse permutation produkt af de samme faktorer blot taget i modsat rækkefølge, da enhver 2-cykel er sin egen invers. Så hvis en permutation kan skrives som produkt af både et lige og et ulige antal 2-cykliske permutationer da må den identiske permutation kunne skrives som et produkt af et ulige antal faktorer, da vi kan skrive permutationen selv som produkt af et lige antal og den inverse som produkt af et ulige antal. Men dette vil jo være en modstrid.

Vi bemærker at faktoriseringen i 2-cykler på ingen måde i sig selv er entydig, men som vi lige har vist så har denne faktorisering dog en entydig egenskab, nemlig pariteten af antallet af faktorer, altså om dette antal er lige eller ulige. Dette er baggrunden for at tildele permutationer paritet og fortegn.

4: Lige eller ulige

På baggrund af sætning S21

4.1: Definition og beregning af fortegn

Med sætning S21 har vi da gjort klar til

---

22. Definition: Paritet, fortegn

En permutation kaldes lige, når den er produkt af et lige antal 2-cykliske permutationer og den siges at have fortegnet 1*. I modsat fald kaldes den ulige og dens fortegn defineres til at være* -1*. Vi skriver* $\operatorname{sgn}(p)$ *for fortegnet af* p*.*

Ved beregning af pariteten for en permutation er det ofte smart at bryde den ned i faktorer som man kan bestemme fortegnet for. Man har nemlig følgende bekvemme hjælpemiddel

23. Sætning: Regning med fortegn

For permutationerne p *og* q *af* A *gælder regnereglen*

$$\operatorname{sgn}(pq) = \operatorname{sgn}(p)\operatorname{sgn}(q),$$

hvilket også betyder at man regner med pariteter på samme måde som hos hele tal.

Bevis : *Hvis* $p = p_1 \cdots p_r$ *og* $q = q_1 \cdots q_s$ *er faktoriseringer i 2-cykliske permutationer da har vi at* $pq = p_1 \cdots p_r q_1 \cdots q_s$ *og dermed at*

$$\operatorname{sgn}(p) = (-1)^r$$
$$\operatorname{sgn}(q) = (-1)^s$$
$$\operatorname{sgn}(pq) = (-1)^{r+s}$$

hvoraf påstanden fremgår.

Beregningen af de enkelte faktorers fortegn foretages ved hjælp af

24. Sætning: Fortegn for cykler

En k-cykel er lige hvis k er ulige og den er ulige hvis k er lige.

Bevis : Dette følger af den formel som indgår i beviset for at en cyklisk permutation er produkt af 2-cykler, hvilket er indledningen til bevist for at enhver permutation er et sådant produkt.

De foregående resultater kan sammenfattes i

25. Sætning: Effektiv formel til beregning af fortegn

En permutation har samme paritet som antallet af cykliske permutationer, hvor antallet af elementer i cyklen er lige, i en faktorisering af permutationen i disjunkte cykler

4.2: Orden

26. Sætning: Forberedelse til definitionen af orden

Lad p være en permutation af A og antag at A har n elementer. Da findes et tal m således at $p^m = (\,)$.

Bevis : Lad først p være en k-cykel. Da er $p^m = ()$ *hvis k går op i m. Lad da* $k_1, \ldots, k_r$ *være længderne af de cykliske faktorer i en faktorisering af p; da vil* $p^m = ()$ *hvis* $m = k_1 \cdots k_r$

27. Definition: Orden af permutation

Det mindste positive tal m for hvilket $p^m = (\,)$ *kaldes ordenen af p.*

28. Sætning: Orden af cykel

En k-cykel har orden k

29. Sætning: Formel for ordenen

Ordenen af en permutation er det mindste tal, der har den egenskab at enhver længde af en cykel der indgår i faktoriseringen i disjunkte cykler, går op i det, kort sagt mindste fælles multiplum af indgående cykellængder. Og med symboler: hvis $p = p_1 \cdots p_m$ *er faktorisering i disjunkte cykler og hvis* l_i *er længden af* p_i *da er ordenen af* p *lig med* $\mathrm{mfm}(l_1, \ldots, l_m)$

Ø12 Ø13 Ø14 Ø15

5: Epilog

Vi har set to eksempler på faktoriseringer af permutationer i særlig simple permutationer, hvor de simple permutationer er de cykliske. Der er to nyttige faktoriseringer:

1) Faktorisering i disjunkte cykler. Denne faktorisering er i det væsentlige entydig og har lighed med primfaktorisering for hele tal.
2) Faktorisering i 2-cykler. Denne faktorisering er langt fra entydig og cyklerne er ikke disjunkte. Det er denne faktorisering som er grundlaget for inddelingen i lige og ulige cykler. Selvom faktoriseringen ikke er entydig, så er der en egenskab ved den som er entydig, nemlig pariteten af antallet af faktorer.

Definitionen af pariteten af en permutation bygger direkte på faktoriseringen i 2-cykler og udtrykkes også i tildelingen af et fortegn til enhver permutation. Dette fortegn har mange anvendelser. Der er simple regler for beregning af fortegnet for en sammensætning af permutationer ud fra fortegnene for de indgående permutationer.

Disse regler består i på at permutationernw erstattes af deres fortegn og sammensætning erstattes af multiplikation. Derved er den afbildning der til en permutation knytter dens fortegn et eksempel på det, der i abstrakt algebra kaldes en homomorfi.

Mange af de anvendte begreber har også mening for vilkårlige bijektive afbildninger. Det der er specielt knyttet til kravet om endelig definitionsmængde er resultaterne knyttet til faktorisering.

6: Eksempler og øvelser

Eksempel 1: Simpelt eksempel fra geometri 1
Lad A være mængden bestående af de tre hjørner X, Y, Z i en ligesidet trekant. En drejning på 120 grader om dennes tyngdepunkt vil da give anledning til en permutation af A, som kan noteres

$$\begin{pmatrix} X & Y & Z \\ Y & Z & X \end{pmatrix},$$

med en passende orientering.

Øvelse 2: Simpelt eksempel fra geometri 2
Opskriv den permutation som fremkommer ved en spejling i højden gennem X

Øvelse 3: Simpelt eksempel fra geometri 3
Beskriv den permutation som fremkommer ved en drejning på 90 grader af hjørnerne i et kvadrat

---

Øvelse 4: Tetraederets drejninger som permutationer
Lad hjørnerne i et regulært tetraeder have betegnelserne $0, 1, 2, 3$. Angiv samtlige drejninger af tretraederet som permutationer af hjørnerne.

Øvelse 5: Modsat side
Lad $M = \{1, 2, 3, 4, 5, 6\}$ og lad $f(x) = 7 - x$ være forskrift for en funktion $f : M \to M$. Vis at f er en permutation.

Øvelse 6: Springertur
Lad M være skakfelterne på et sædvanligt skakbræt. Find en permutation f af M således at man for alle felter x kan komme fra x til $f(x)$ med et springertræk.

Øvelse 7: Bland kortene
Fortolk kortblanding som en permutation.

Øvelse 8: Baner for tetraederdrejningerne
Forsættelse af Ø4. Vælg et hjørnepunkt og en drejning og beskriv banen.

Øvelse 9: Beregning af produkt ved brug af faktorisering
Vi betragter $p = (136)(45)$, $q = (12)(56)$ og $r = (1234)(56)$ og vil illustrere beregningen af $pqr(1)$. Vi har at

$$pqr = (136)(45)(12)(56)(1234)(56),$$

og vi ønsker at skrive pqr som produkt af disjunkte cykler. Den bagerste faktor som gør noget ved $a = 1$ er (1234), som giver resultatet $b = 2$. Den bagerste foranstående som gør noget ved $b = 2$ er (12) som giver resultatet 1. Den bagerste foranstående som virker på 1 er (136) som giver resultatet 3. Det samlede resultat er derfor at $pqr(1) = 3$. Vi forsætter derefter med på samme måde at bestemme $pqr(3)$ osv.

Øvelse 10: Faktorisering af tetraederdrejningerne
Fortsættelse af Ø4. Opskriv drejningerne af tetrederet som produkt af dijunkte cykler.

Øvelse 11: Faktorisering af terningens drejninger som permutationer af hjørnerne
Lad hjørnerne i en enhedsterningen være nummereret således at koordinaterne x, y og z til et punkt er de binære cifre i nummeret, x det mindst betydende og z det mest betydende. Eksempelvis vil $(0, 1, 1)$ have nummeret $6 = 0{\cdot}1{+}1{\cdot}2{+}1{\cdot}4$. Angiv nogle typiske drejninger som permutationer af hjørnerne og find deres faktoriseringer i disjunkte cykler.

Øvelse 12: Faktorisering af terningens drejninger som permutationer af siderne
Lad siderne på en terning være nummeret fra 1 til 6 i overensstemmelse med antallet af øjne. Lad et koordinatsystem have begyndelsespunkt i terningens centrum og lad enhedspunkterne på x, y, z-akserne være midtpunkterne på siderne med numrene $1, 2, 3$ Antag at dette system er højrehåndet. Lad X være den permutation af siderne som svarer til en drejning 90 om x-aksen. Tilsvarende for de andre akser. Lad I betegne den permutation der svarer til ombytning af modstående sider. Opskriv disse permutationer i de forskellige notationer. Gør det samme med XY, YX, XYX, IX, XI, XIX. Beregn paritet og orden for hver af disse permutationer.

Øvelse 13: Faktorisering af terningens drejninger som permutationer af diagonaler
Fortsættlese af Ø12.

Formuler og løs en lignende opgave for hjørner og for diagonaler.

Øvelse 14: Affin modulær funktion som permutation
Vi benytter betegnelsen $a \bmod b$ for resten ved division af a med b, altså $7 \bmod 5 = 2, 18 \bmod 5 = 3$.

Lad $A = \{0, 1, 2, 3, 4, 5\}$. Vis at forskriften $f(x) = (5x + 2) \bmod 6$ definerer en permutation af A. Angiv dens orden.

Undersøg hvilke af afbildningerne $f(x) = 5x + a \bmod 6$, hvor a er en konstant der giver anledning til en permutation.

Øvelse 15: Disjunkte cykler kommuterer
To permutationer p og q med disjunkte støtter vil kommutere, dvs $pq = qp$.
